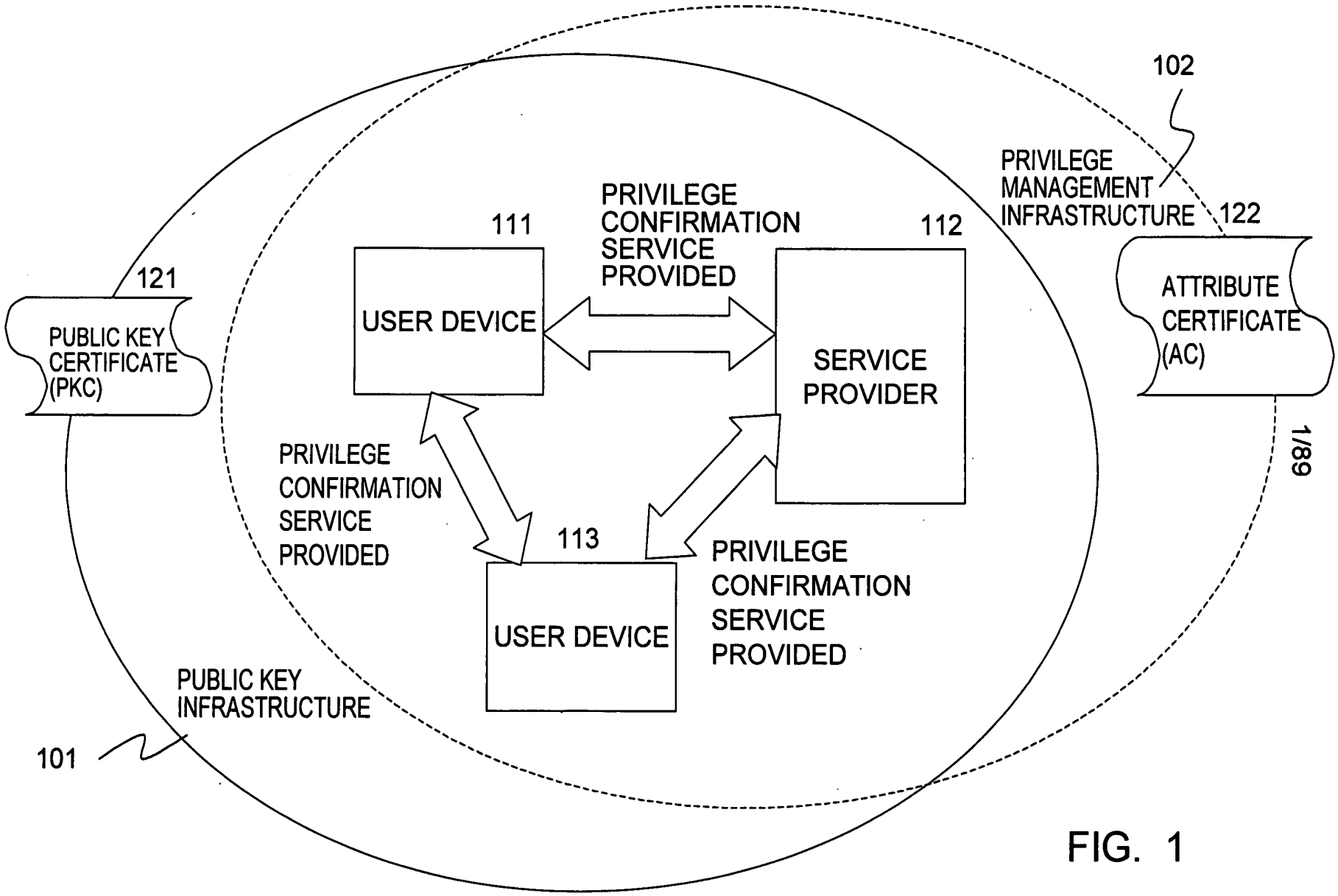


FIG. 1

VERSION	ITEM	DESCRIPTION
V-1	VERSION	VERSION OF FORMAT OF CERTIFICATE
	SERIAL NUMBER	CERTIFICATE NUMBER ASSIGNED BY CERTIFICATE ISSUER
	SIGNATURE	SIGNATURE ALGORITHM OF CERTIFICATE
	ISSUER	NAME OF CERTIFICATE ISSUER (DISTINGUISHED NAME FORMAT)
	VALIDITY START END	PERIOD IN WHICH CERTIFICATE IS VALID STARTING DATE AND TIME ENDING DATE AND TIME
	SUBJECT	NAME OF HOLDER OF CERTIFICATE
	SUBJECT PUBLIC KEY INFORMATION ALGORITHM SUBJECT PUBLIC KEY	PUBLIC KEY INFORMATION OF HOLDER OF CERTIFICATE ALGORITHM OF KEY KEY

FIG. 2

V-3	AUTHORITY KEY IDENTIFIER KEY IDENTIFIER AUTHORITY CERTIFICATE ISSUER NAME AUTHORITY CERTIFICATE SERIAL NUMBER	KEY IDENTIFIER OF CERTIFICATE ISSUER USED FOR SIGNATURE VERIFICATION KEY IDENTIFIER ORGANIZATION CERTIFICATE ISSUER NAME (GENERAL NAME FORMAT) ORGANIZATION CERTIFICATE SERIAL NUMBER
	SUBJECT KEY IDENTIFIER KEY IDENTIFIER	CLEARLY IDENTIFY OBJECT KEY FROM MULTIPLE KEYS
	KEY USAGE (0) DIGITAL SIGNATURE (1) NON-REPUDIATION (2) KEY ENCIPHERMENT (3) DATA ENCIPHERMENT (4) KEY AGREEMENT (5) KEY CERT SIGNATURE (6) cRL SIGNATURE	SPECIFY USAGE OF KEY (0) FOR DIGITAL SIGNATURE (1) FOR PREVENTING REPUDIATION (2) FOR ENCIPHERING KEY (3) FOR ENCIPHERING MESSAGE (4) FOR DISTRIBUTING SHARED KEY (5) FOR CONFIRMING SIGNATURE OF CERTIFICATION (6) FOR CONFIRMING SIGNATURE OF REVOCATION LIST
	SECRET KEY VALIDITY START END	VALID PERIOD FOR SECRET KEY CORRESPONDING TO PUBLIC KEY IN CERTIFICATE
	CERTIFICATE POLICY POLICY IDENTIFIER POLICY QUALIFIER	CERTIFICATE POLICY ACKNOWLEDGED BY CERTIFICATE ISSUER POLICY ID (ISO/IEC9834-1 COMPLIANT) AUTHENTICATION STANDARD
	POLICY MAPPING ISSUER DOMAIN POLICY SUBJECT DOMAIN POLICY	RESTRICTION OF RELATION OF POLICIES IN AUTHENTICATION PATH

FIG. 3

V-3	SUBJECT ALTERNATE NAME	ALTERNATIVE NAME FOR CERTIFICATE HOLDER (GN FORMAT)
	ISSUER ALTERNATIVE NAME	ALTERNATIVE NAME FOR CERTIFICATE ISSUER(GN FORMAT)
	SUBJECT DIRECTORY ATTRIBUTE	ATTRIBUTE OF DIRECTORY NECESSARY FOR CERTIFICATE HOLDER
	BASIC CONSTRAINT CA PATH LENGTH CONSTRAINT	DISTINGUISH WHETHER PUBLIC KEY FOR CERTIFICATION IS FOR SIGNATURE OF CERTIFYING AUTHORITY, OR BELONGS TO CERTIFICATE HOLDER
	NAMING CONSTRAINT PERMITTED SUBTREES BASE MINIMUM MAXIMUM EXCLUSION CONSTRAINT	RESTRICTS NAME OF CERTIFICATE ISSUED BY ISSUER
	POLICY CONSTRAINT REQUIRE EXPLICIT POLICY INHIBIT POLICY MAPPING	RESTRICTS RELATIONS OF POLICIES IN AUTHENTICATION PATH
	CRL DISTRIBUTION POINT	DESCRIBES DISTRIBUTION POINTS OF REVOCATION LIST FOR CONFIRMING WHETHER OR NOT CERTIFICATE HAS BEEN REVOKED AT TIME OF CERTIFICATE HOLDER USING CERTIFICATE
	SIGNATURE ALGORITHM	ALGORITHM USED FO ATTACHING SIGNATURE TO CERTIFICATE
	SIGNATURE VALUE	SIGNATURE BY SECRET KEY OF CERTIFICATE ISSUER

FIG. 4

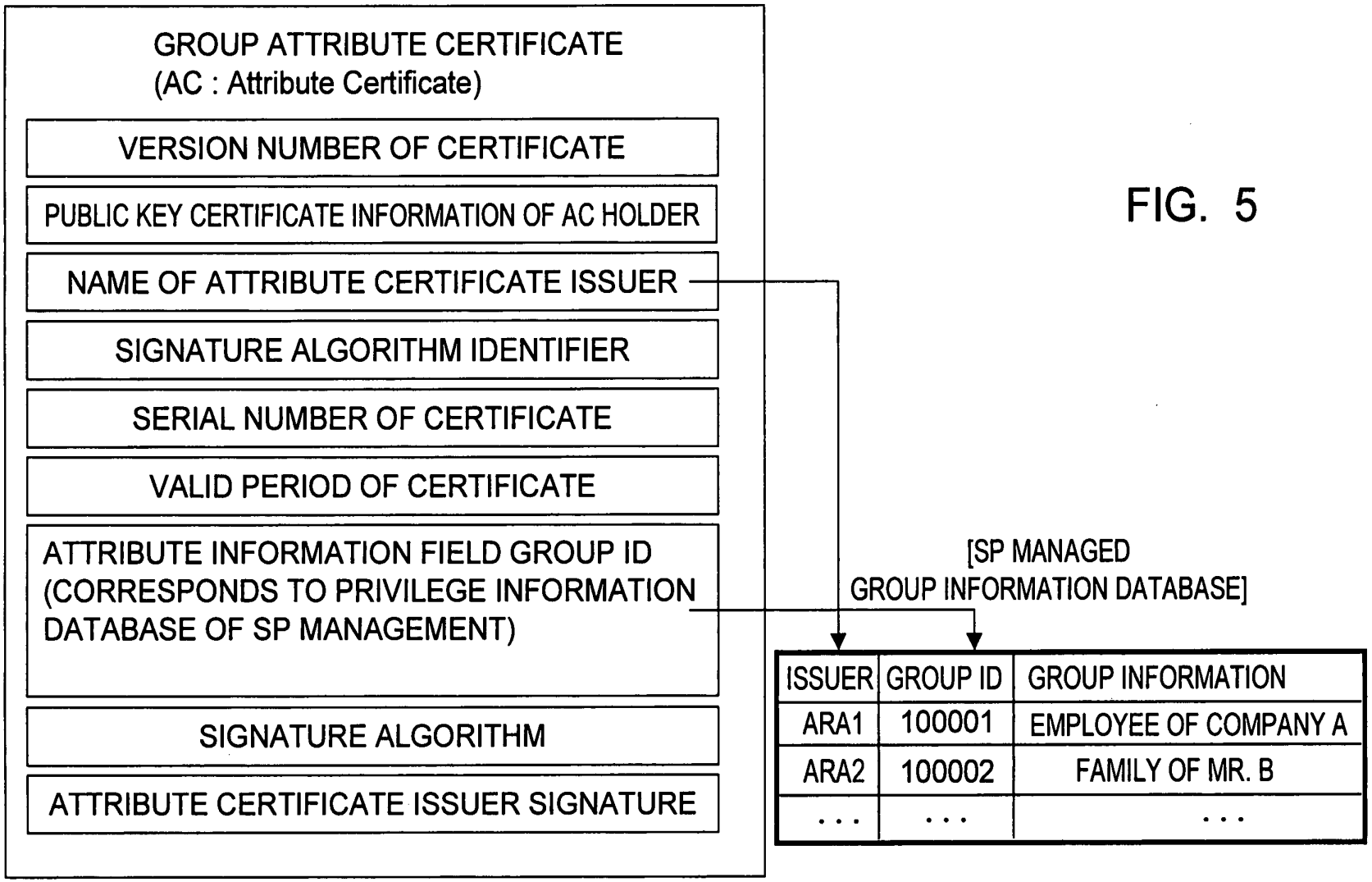


FIG. 5

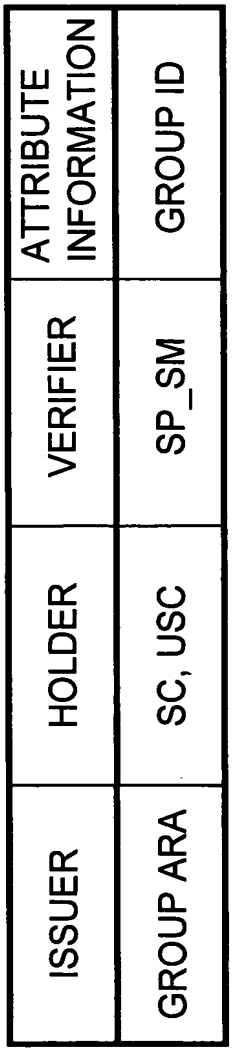

ISSUER
HOLDER
VERIFIER
ATTRIBUTE INFORMATION
GROUP ARA
SC, USC
SP_SM
GROUP ID

FIG. 6

GROUP ID	GROUP INFORMATION	ISSUING POLICY
1234-0	GAME DISTRIBUTION SERVICE MEMBER	• OWNS AUTHORIZED GAME MACHINE CONFIRMED WITH EE PKC, ETC • ALREADY PAID GAME DISTRIBUTION SERVICE JOINING FEE
1234-5-10	10-GAME USAGE MEMBER	• MEMBER OF GAME DISTRIBUTION SERVICE OWNS GAME DISTRIBUTION SERVICE MEMBER AC • AGREED TO LIMIT TO 10 TIMES
. . .	. . .	. . .

FIG. 7

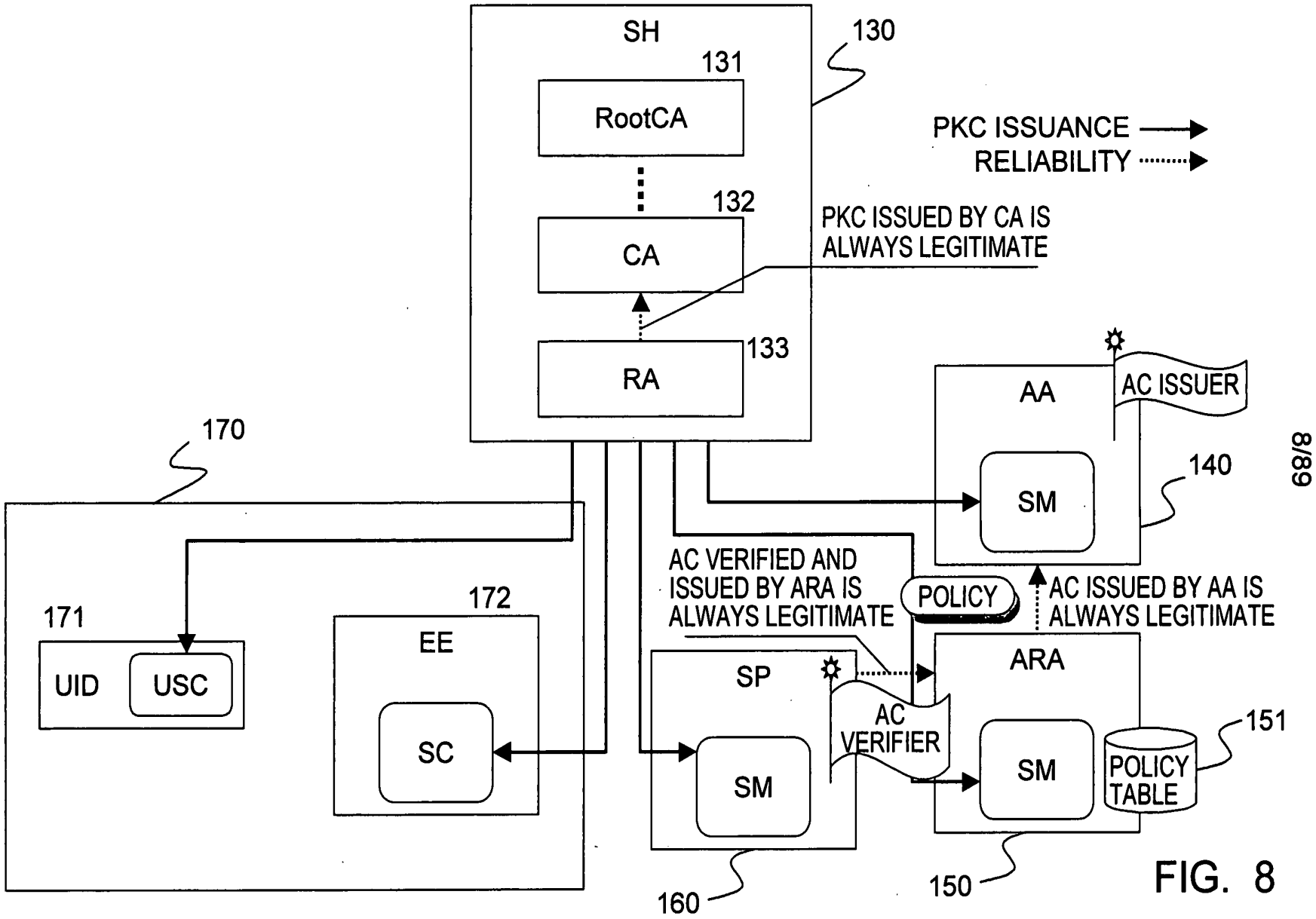


FIG. 8

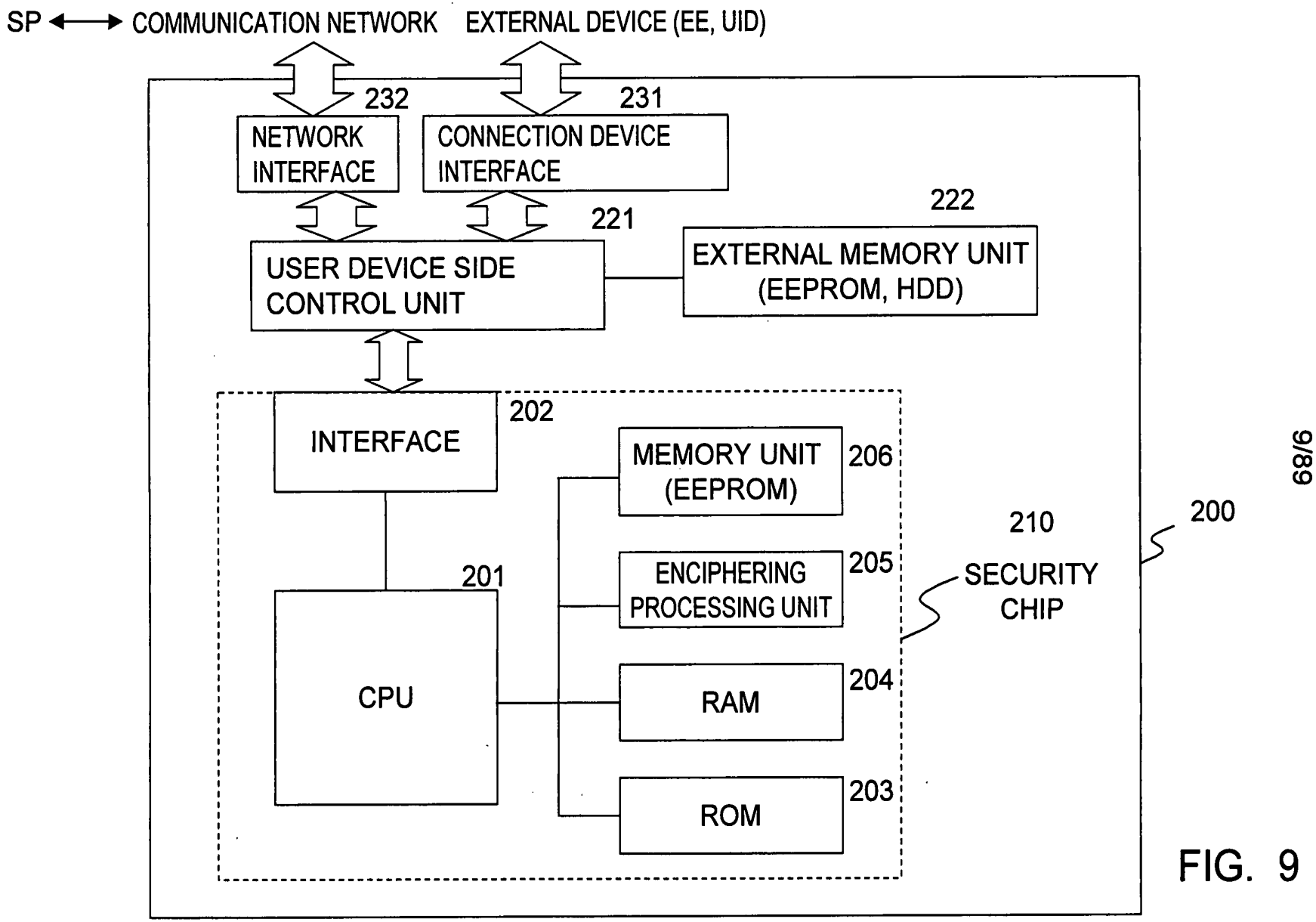

SP
COMMUNICATION NETWORK
EXTERNAL DEVICE (EE, UID)
232
231
NETWORK INTERFACE
CONNECTION DEVICE INTERFACE
222
221
USER DEVICE SIDE CONTROL UNIT
EXTERNAL MEMORY UNIT (EEPROM, HDD)
202
INTERFACE
MEMORY UNIT (EEPROM)
206
210
200
201
ENCIPHERING PROCESSING UNIT
205
SECURITY CHIP
CPU
204
RAM
203
ROM

FIG. 9

DATA TYPE	DATA CONTENTS
PUBLIC KEY CERTIFICATE	• ROUTE CERTIFICATION AUTHORITY PUBLIC KEY CERTIFICATE • SERVICE PROVIDER PUBLIC KEY CERTIFICATE
GROUP ATTRIBUTE CERTIFICATE	• ATTRIBUTE CERTIFICATE CORRESPONDING TO GROUP TO WHICH DEVICE BELONGS OR USER BELONGS
EXECUTION ATTRIBUTE CERTIFICATE	• ATTRIBUTE CERTIFICATE CONTAINING ADDRESS DATA OF MEMORY STORING ENCIPHERING COMMAND AND DECIPHERING REGISTRATION KEY OF ENCIPHERING COMMAND
KEY DATA	• SECURITY CHIP PUBLIC KEY, SECRET KEY PAIR • REGISTRATION KEY • RESET KEY • RANDOM NUMBER GENERATING KEY, • MUTUAL AUTHENTICATION KEY
IDENTIFICATION INFORMATION	• SECURITY CHIP ID • SERVICE PROVIDER ID • USER ID • APPLICATION ID
OTHERS	• RANDOM NUMBER SEED • SERVICE USAGE INFORMATION, ETC.

FIG. 10

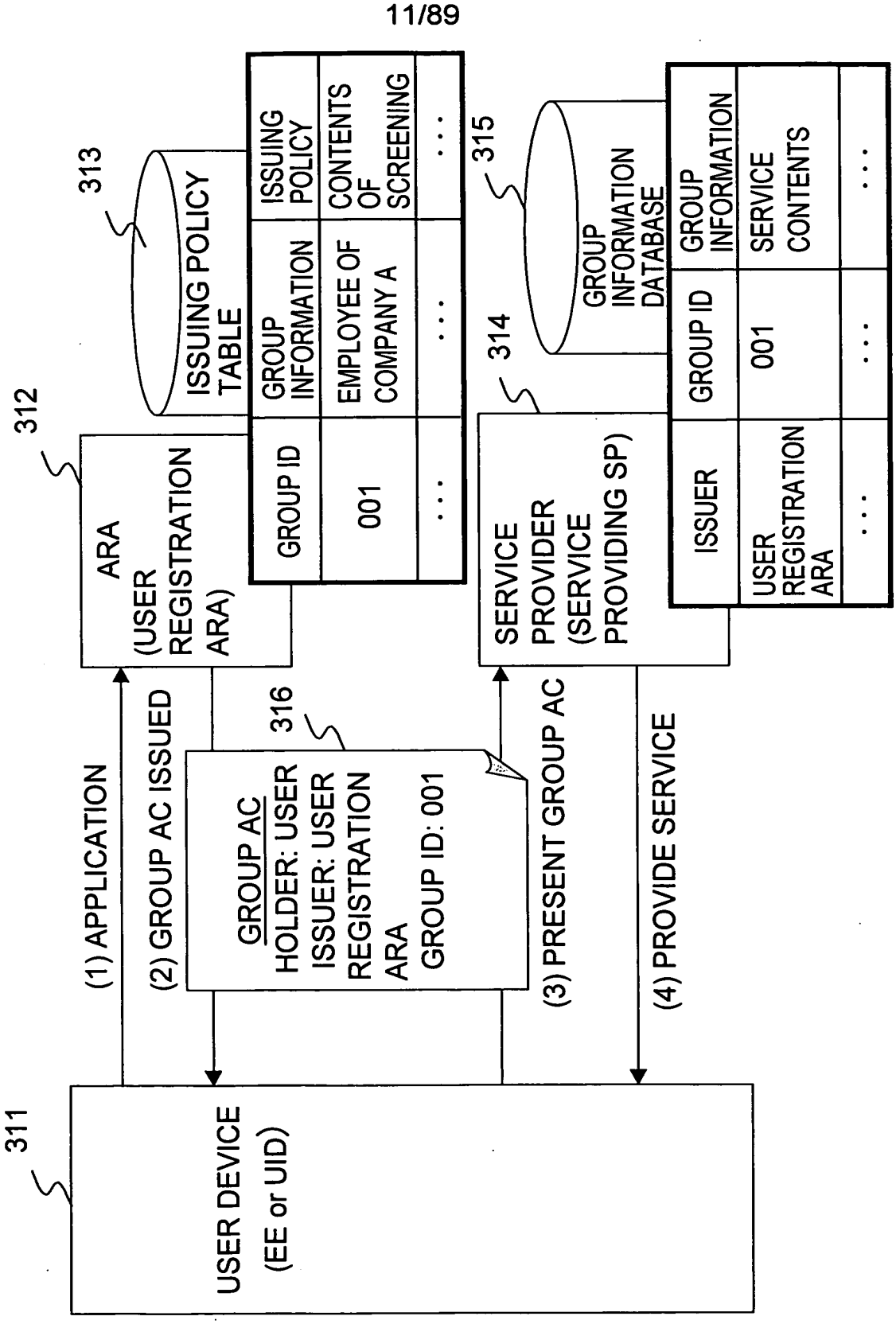

311
USER DEVICE
(EE or UID)
312
ARA
(USER REGISTRATION ARA)
313
ISSUING POLICY TABLE
GROUP ID
001
GROUP INFORMATION
EMPLOYEE OF COMPANY A
ISSUING POLICY
CONTENTS OF SCREENING
314
SERVICE PROVIDER
(SERVICE PROVIDING SP)
315
GROUP INFORMATION DATABASE
ISSUER
USER REGISTRATION ARA
GROUP ID
001
GROUP INFORMATION
SERVICE CONTENTS
316
GROUP AC
HOLDER: USER
ISSUER: USER REGISTRATION ARA
GROUP ID: 001
(1) APPLICATION
(2) GROUP AC ISSUED
(3) PRESENT GROUP AC
(4) PROVIDE SERVICE

FIG. 11

FIG. 12

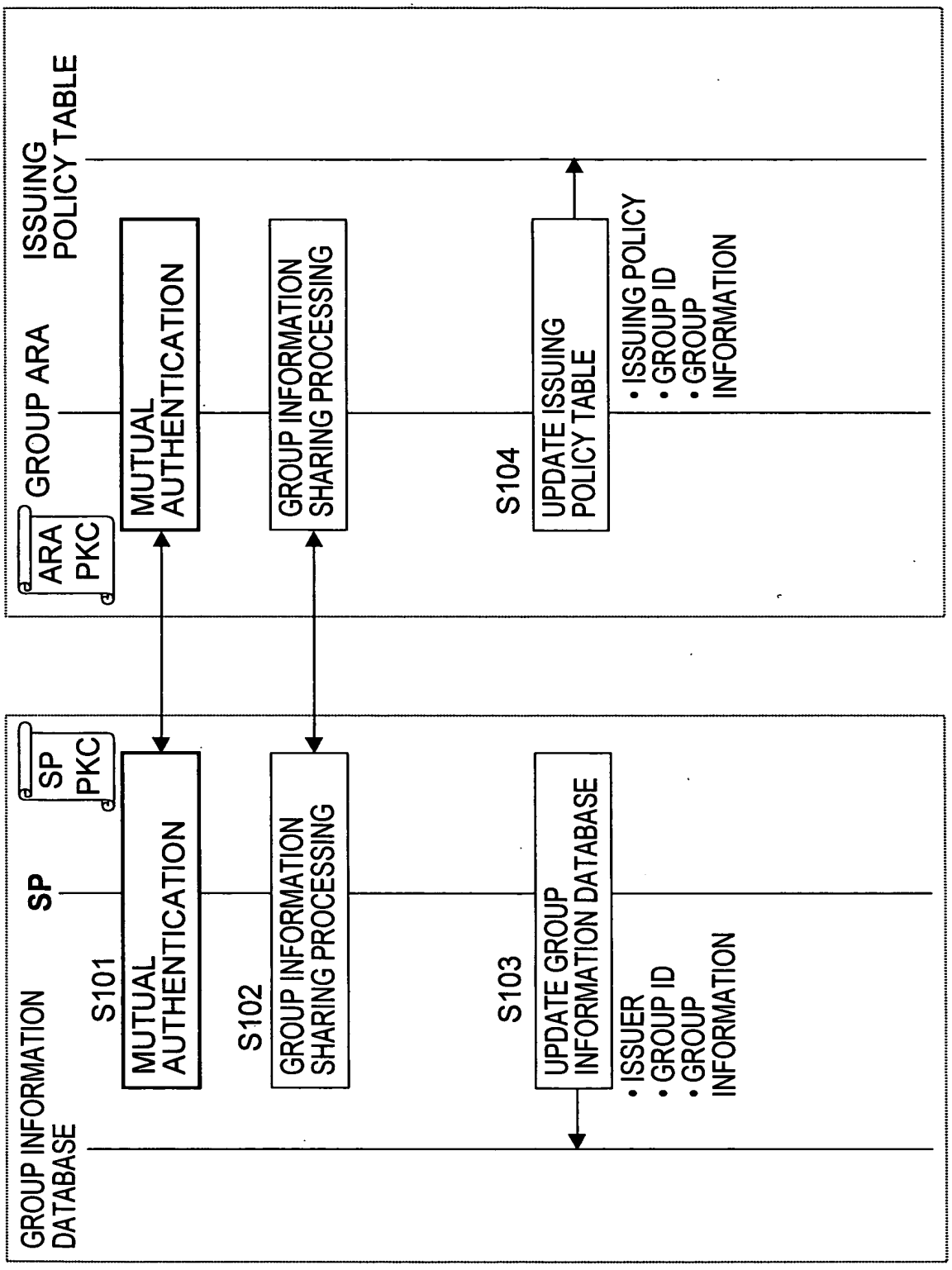
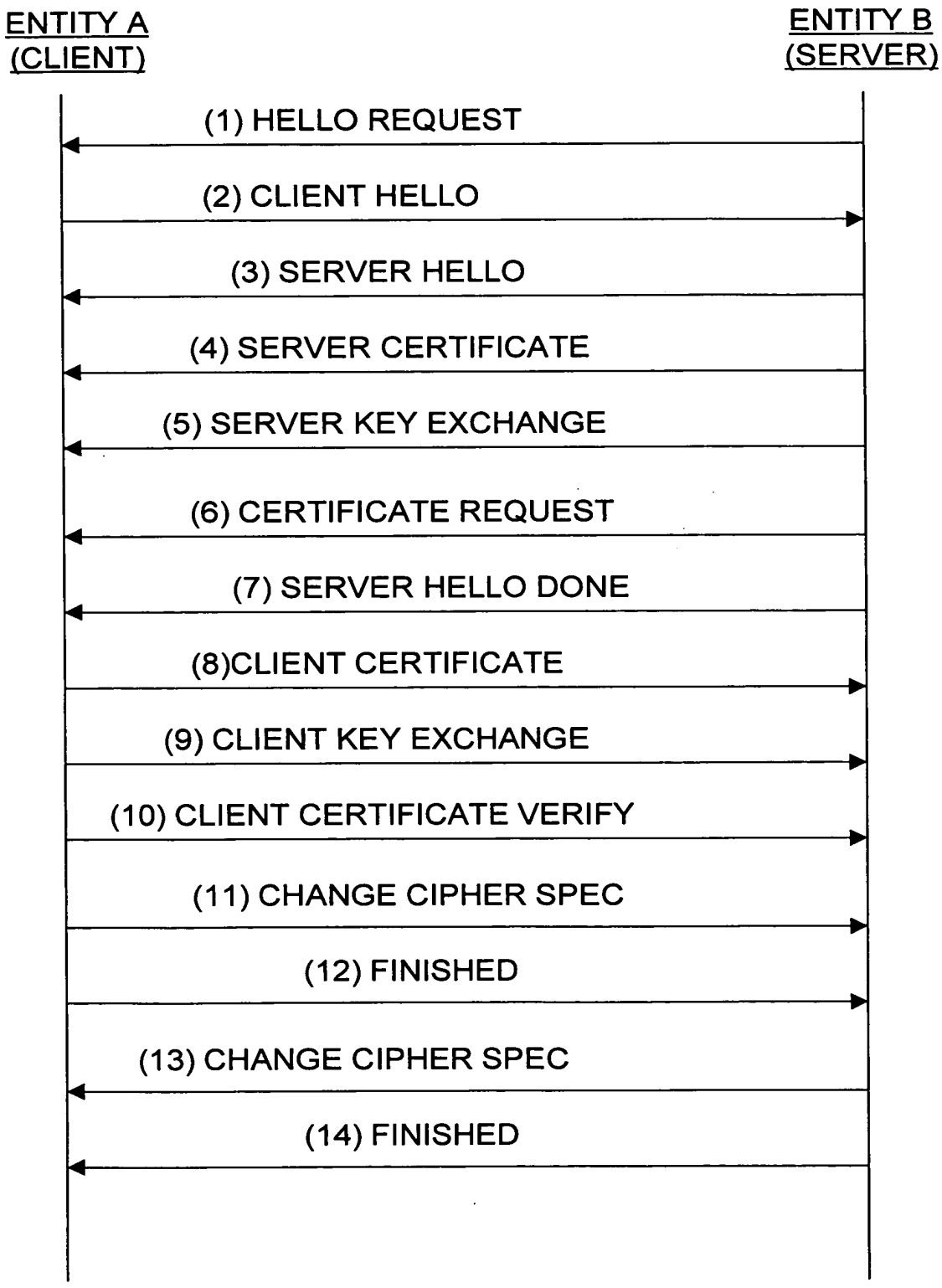

GROUP INFORMATION DATABASE
SP
SP PKC
S101
MUTUAL AUTHENTICATION
S102
GROUP INFORMATION SHARING PROCESSING
S103
UPDATE GROUP INFORMATION DATABASE
• ISSUER
• GROUP ID
• GROUP INFORMATION
GROUP ARA
ARA PKC
MUTUAL AUTHENTICATION
GROUP INFORMATION SHARING PROCESSING
S104
UPDATE ISSUING POLICY TABLE
ISSUING POLICY TABLE
• ISSUING POLICY
• GROUP ID
• GROUP INFORMATION

FIG. 13


ENTITY A
(CLIENT)
ENTITY B
(SERVER)
(1) HELLO REQUEST
(2) CLIENT HELLO
(3) SERVER HELLO
(4) SERVER CERTIFICATE
(5) SERVER KEY EXCHANGE
(6) CERTIFICATE REQUEST
(7) SERVER HELLO DONE
(8)CLIENT CERTIFICATE
(9) CLIENT KEY EXCHANGE
(10) CLIENT CERTIFICATE VERIFY
(11) CHANGE CIPHER SPEC
(12) FINISHED
(13) CHANGE CIPHER SPEC
(14) FINISHED

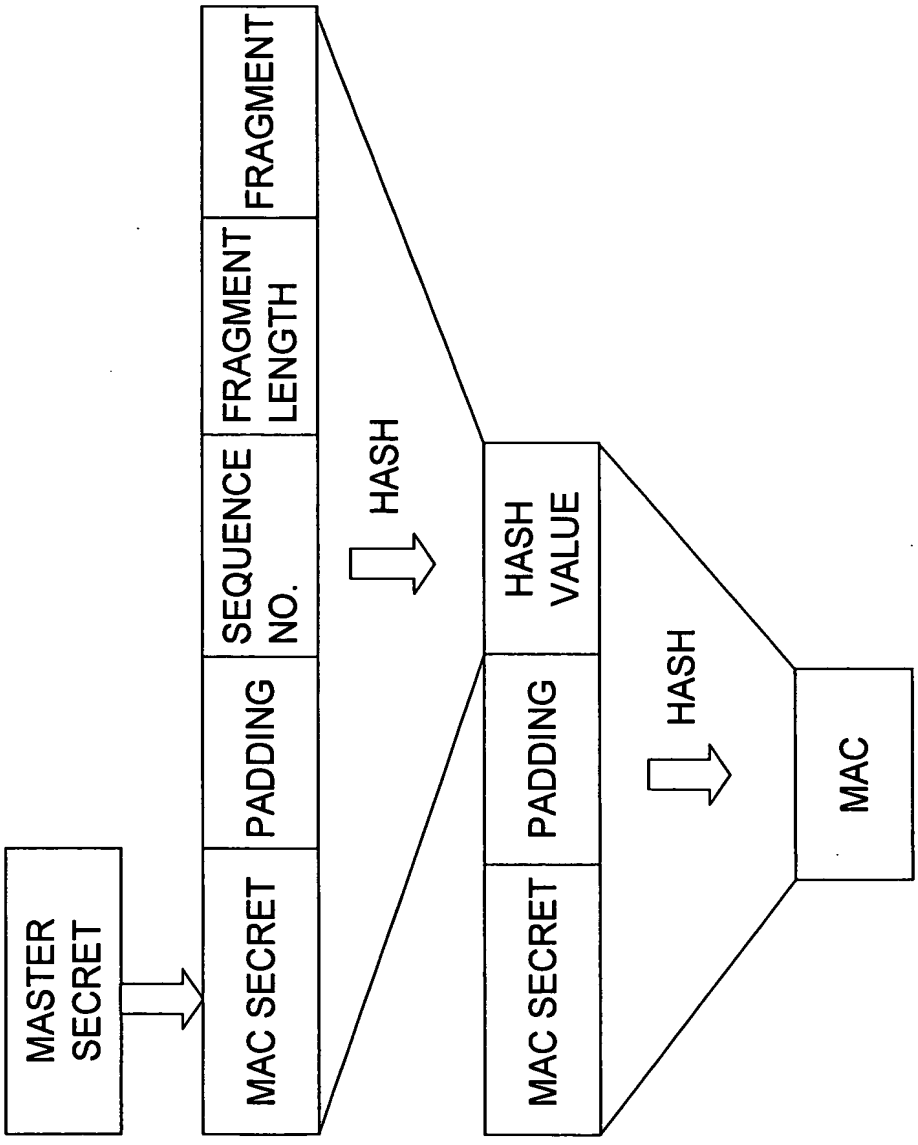

MASTER SECRET
MAC SECRET
PADDING
SEQUENCE NO.
FRAGMENT LENGTH
FRAGMENT
HASH
HASH VALUE
MAC SECRET
PADDING
HASH
MAC

FIG. 14

(A) ISSUING POLICY TABLE (HELD BY ARA)

GROUP ID	GROUP INFORMATION	ISSUING POLICY
1234-0	GAME DISTRIBUTION SERVICE MEMBER	• OWNS AUTHORIZED GAME MACHINE CONFIRMED WITH EE PKC, ETC • ALREADY PAID GAME DISTRIBUTION SERVICE JOINING FEE
1234-5-10	10-GAME USAGE MEMBER	• MEMBER OF GAME DISTRIBUTION SERVICE OWNS GAME DISTRIBUTION SERVICE MEMBER AC • AGREED TO LIMIT TO 10 TIMES

341

342

(B) GROUP INFORMATION DATABASE (HELD BY SP)

ISSUER	GROUP ID	GROUP INFORMATION
MANUFACTURER	1001	MAINTENANCE: FULL-SERVICE SUBSCRIBER
MANUFACTURER	1002	MAINTENANCE: TRIAL
GAME DISTRIBUTION SERVICE	1234-0	GAME DISTRIBUTION SERVICE MEMBER
GAME DISTRIBUTION SERVICE	1234-5-10	10-GAME USAGE MEMBER
TANAKA FAMILY, HEAD	001	TANAKA FAMILY, FAMILY
TANAKA FAMILY, HEAD	002	TANAKA FAMILY, CHILDREN

351

352

FIG. 15

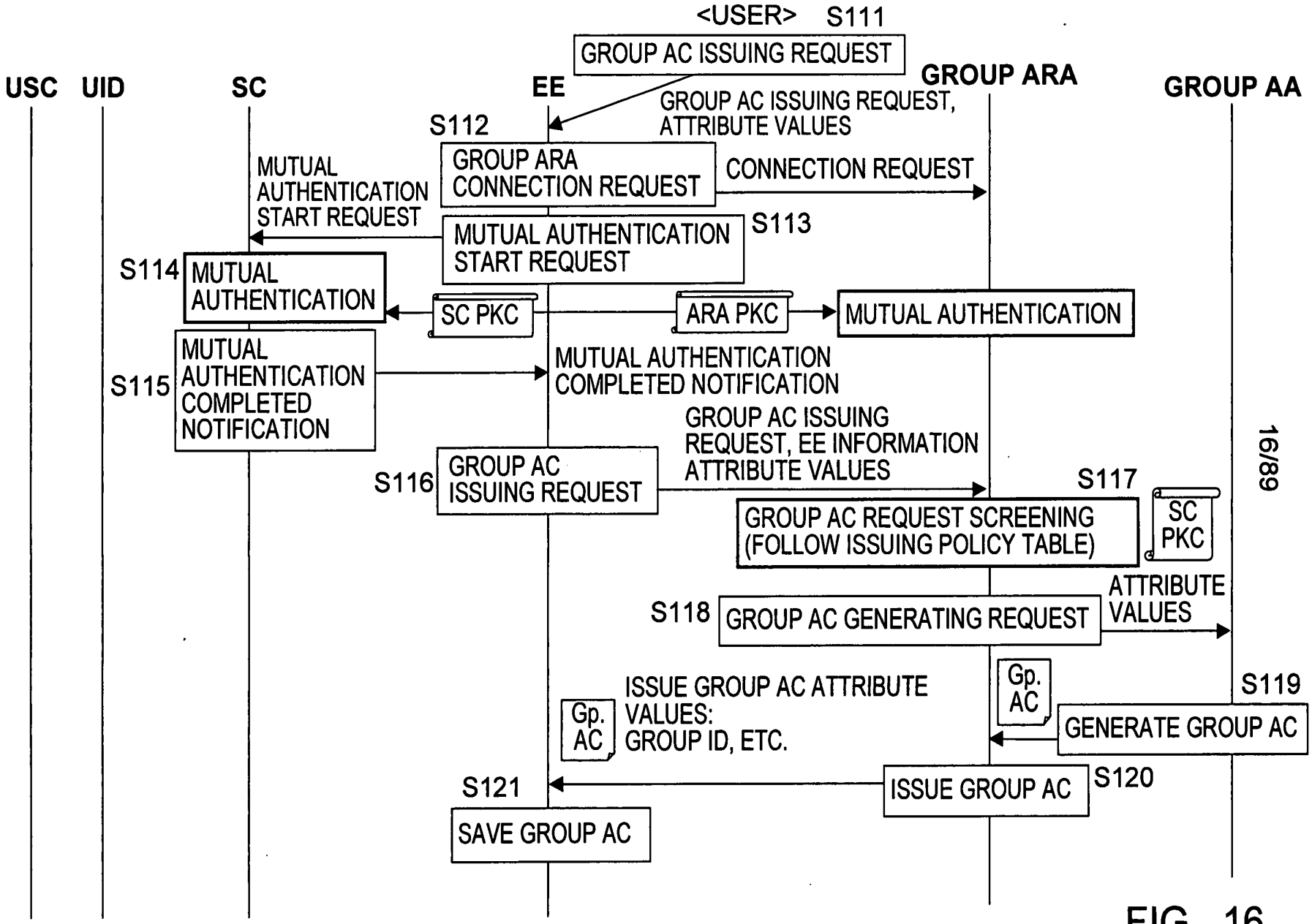


FIG. 16

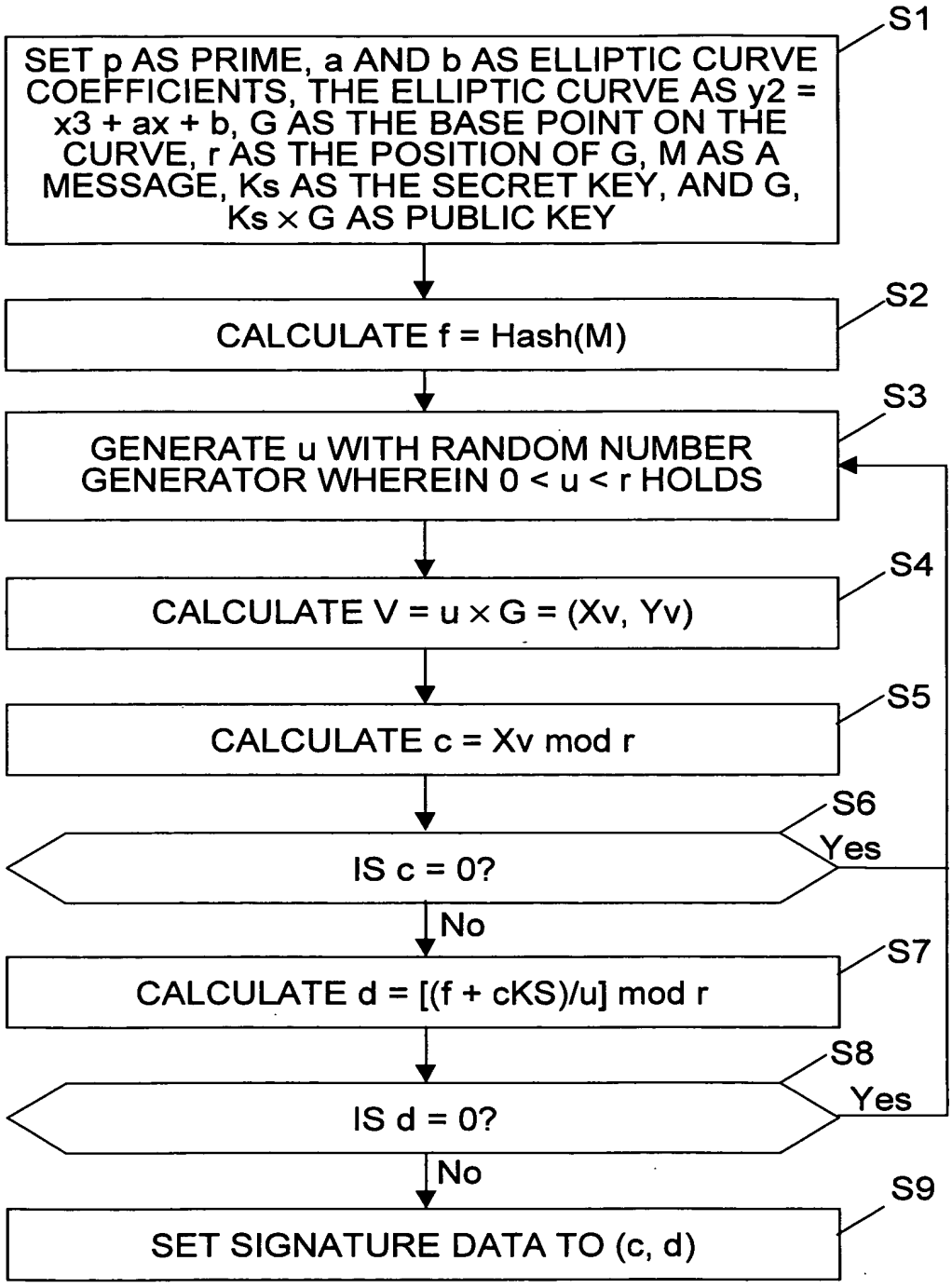

S1
SET p AS PRIME, a AND b AS ELLIPTIC CURVE COEFFICIENTS, THE ELLIPTIC CURVE AS y2 = x3 + ax + b, G AS THE BASE POINT ON THE CURVE, r AS THE POSITION OF G, M AS A MESSAGE, Ks AS THE SECRET KEY, AND G, Ks × G AS PUBLIC KEY
S2
CALCULATE f = Hash(M)
S3
GENERATE u WITH RANDOM NUMBER GENERATOR WHEREIN 0 < u < r HOLDS
S4
CALCULATE V = u × G = (Xv, Yv)
S5
CALCULATE c = Xv mod r
S6
IS c = 0?
Yes
No
S7
CALCULATE d = [(f + cKS)/u] mod r
S8
IS d = 0?
Yes
No
S9
SET SIGNATURE DATA TO (c, d)

FIG. 17

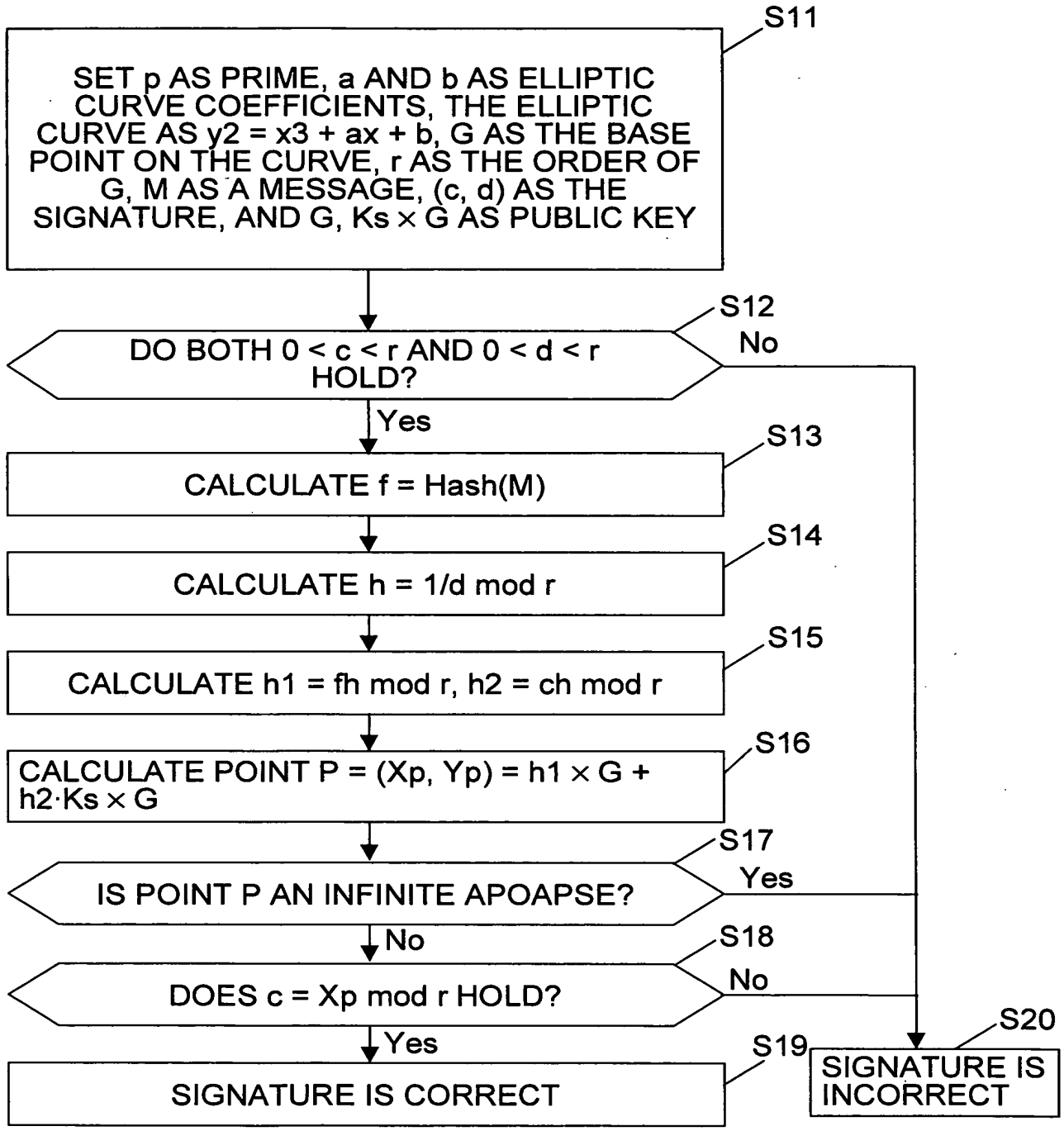

S11
SET p AS PRIME, a AND b AS ELLIPTIC CURVE COEFFICIENTS, THE ELLIPTIC CURVE AS y2 = x3 + ax + b, G AS THE BASE POINT ON THE CURVE, r AS THE ORDER OF G, M AS A MESSAGE, (c, d) AS THE SIGNATURE, AND G, Ks × G AS PUBLIC KEY
S12
DO BOTH 0 < c < r AND 0 < d < r HOLD?
No
Yes
S13
CALCULATE f = Hash(M)
S14
CALCULATE h = 1/d mod r
S15
CALCULATE h1 = fh mod r, h2 = ch mod r
S16
CALCULATE POINT P = (Xp, Yp) = h1 × G + h2·Ks × G
S17
IS POINT P AN INFINITE APOAPSE?
Yes
No
S18
DOES c = Xp mod r HOLD?
No
Yes
S19
SIGNATURE IS CORRECT
S20
SIGNATURE IS INCORRECT

FIG. 18

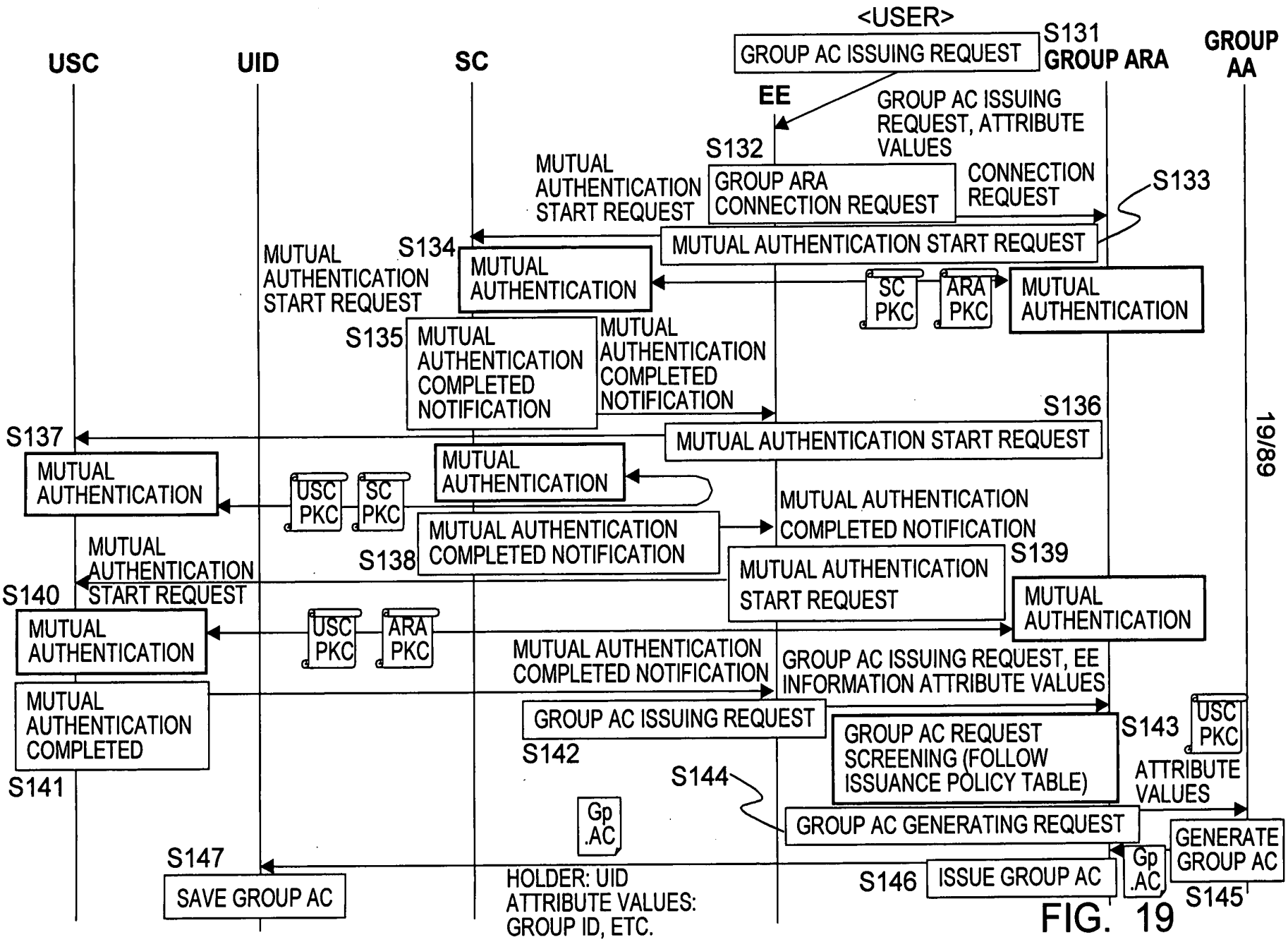


FIG. 19

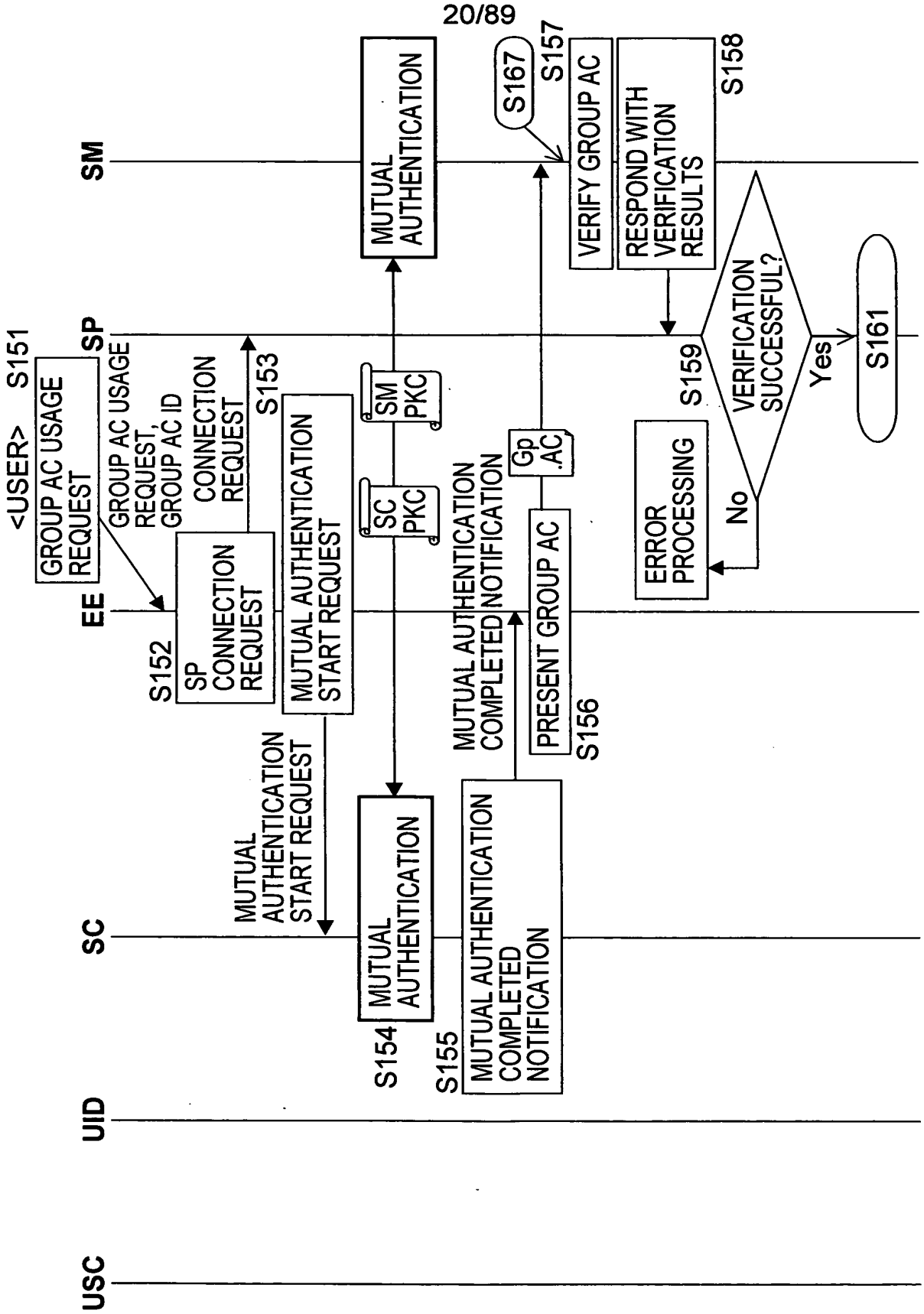

USC
UID
SC
EE
SP
SM
<USER>
S151
GROUP AC USAGE REQUEST
GROUP AC USAGE REQUEST, GROUP AC ID
S152
SP CONNECTION REQUEST
CONNECTION REQUEST
S153
MUTUAL AUTHENTICATION START REQUEST
MUTUAL AUTHENTICATION START REQUEST
SC PKC
SM PKC
S154
MUTUAL AUTHENTICATION
S155
MUTUAL AUTHENTICATION COMPLETED NOTIFICATION
MUTUAL AUTHENTICATION COMPLETED NOTIFICATION
Gp .AC
S156
PRESENT GROUP AC
MUTUAL AUTHENTICATION
S167
S157
VERIFY GROUP AC
S158
RESPOND WITH VERIFICATION RESULTS
S159
VERIFICATION SUCCESSFUL?
No
ERROR PROCESSING
Yes
S161

FIG. 20

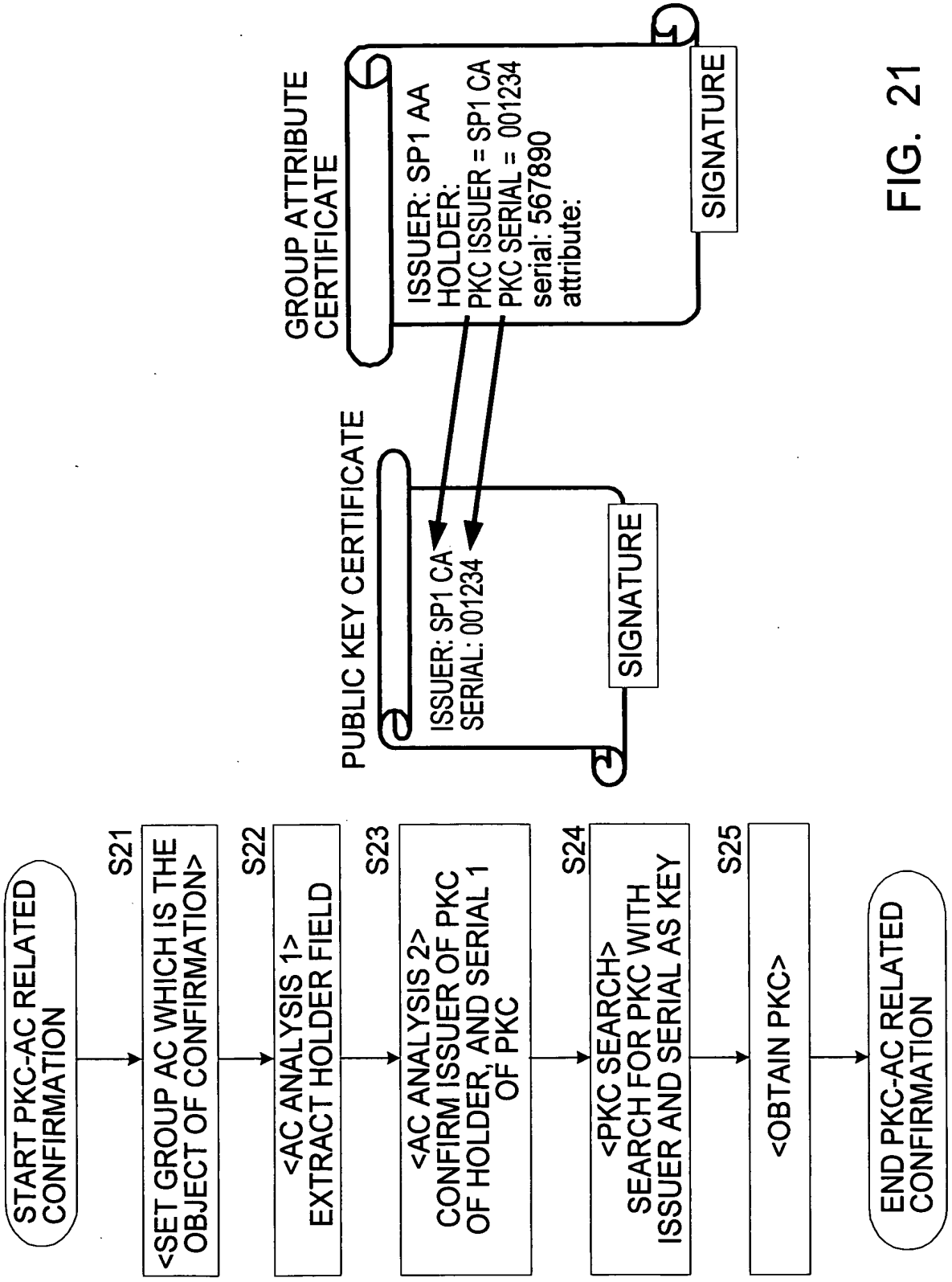

START PKC-AC RELATED CONFIRMATION
S21
<SET GROUP AC WHICH IS THE OBJECT OF CONFIRMATION>
S22
<AC ANALYSIS 1> EXTRACT HOLDER FIELD
S23
<AC ANALYSIS 2> CONFIRM ISSUER OF PKC OF HOLDER, AND SERIAL 1 OF PKC
S24
<PKC SEARCH> SEARCH FOR PKC WITH ISSUER AND SERIAL AS KEY
S25
<OBTAIN PKC>
END PKC-AC RELATED CONFIRMATION
GROUP ATTRIBUTE CERTIFICATE
ISSUER: SP1 AA
HOLDER:
PKC ISSUER = SP1 CA
PKC SERIAL = 001234
serial: 567890
attribute:
SIGNATURE
PUBLIC KEY CERTIFICATE
ISSUER: SP1 CA
SERIAL: 001234
SIGNATURE

FIG. 21

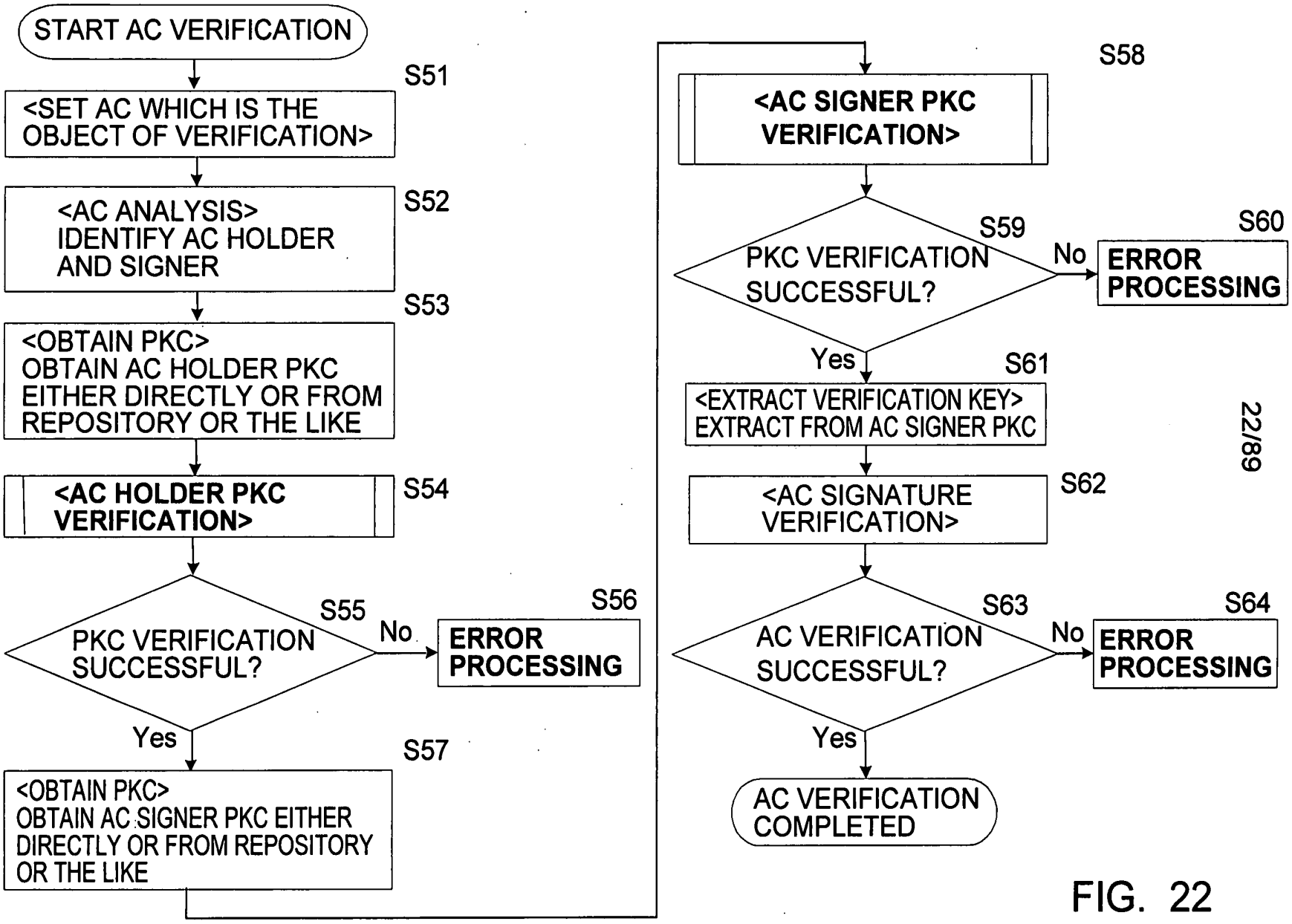


FIG. 22

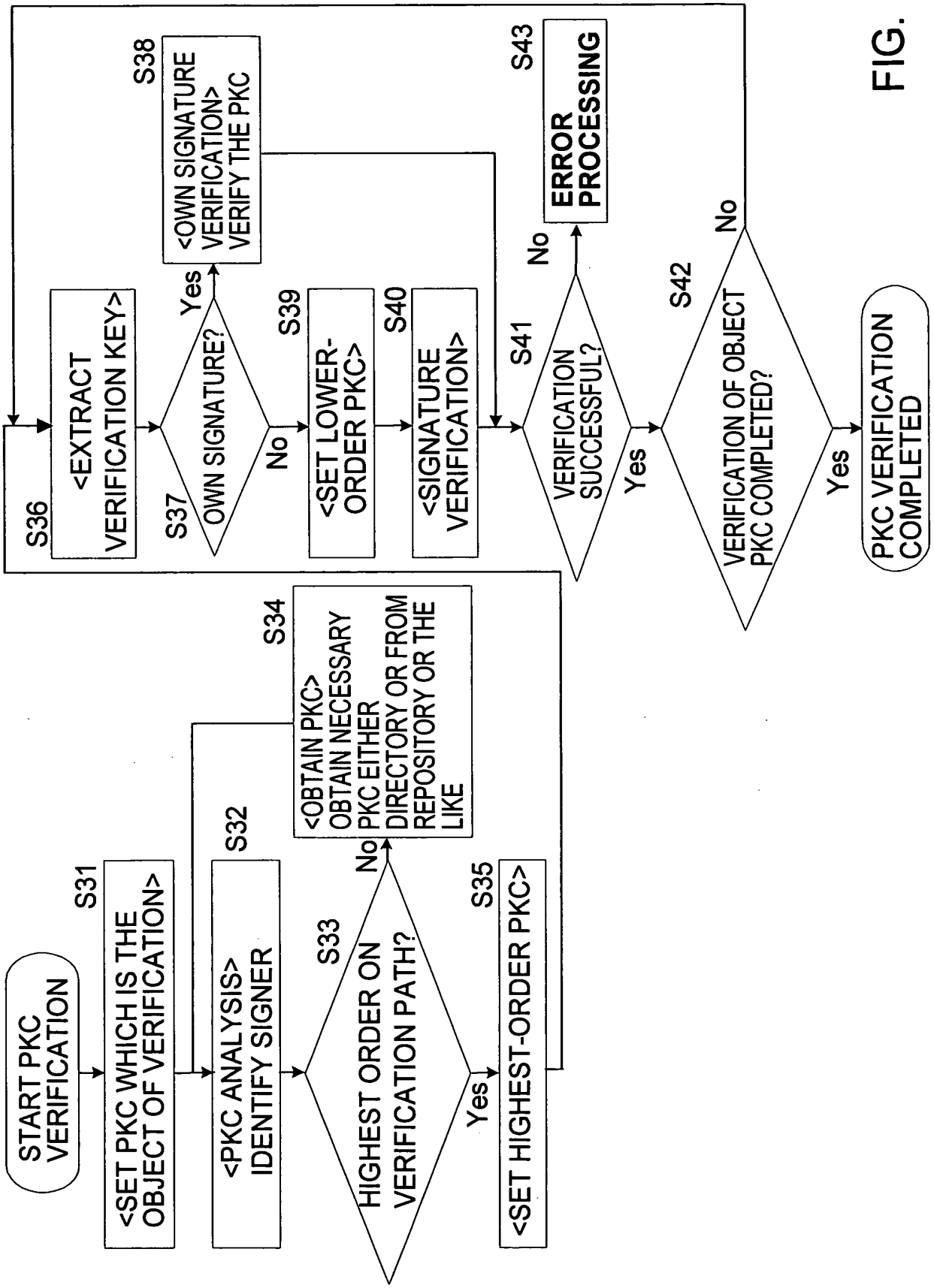

START PKC VERIFICATION
S31
<SET PKC WHICH IS THE OBJECT OF VERIFICATION>
S32
<PKC ANALYSIS> IDENTIFY SIGNER
S33
HIGHEST ORDER ON VERIFICATION PATH?
No
S34
<OBTAIN PKC> OBTAIN NECESSARY PKC EITHER DIRECTORY OR FROM REPOSITORY OR THE LIKE
Yes
S35
<SET HIGHEST-ORDER PKC>
S36
<EXTRACT VERIFICATION KEY>
S37
OWN SIGNATURE?
Yes
S38
<OWN SIGNATURE VERIFICATION> VERIFY THE PKC
No
S39
<SET LOWER-ORDER PKC>
S40
<SIGNATURE VERIFICATION>
S41
VERIFICATION SUCCESSFUL?
No
S43
ERROR PROCESSING
Yes
S42
VERIFICATION OF OBJECT PKC COMPLETED?
No
Yes
PKC VERIFICATION COMPLETED

FIG. 23

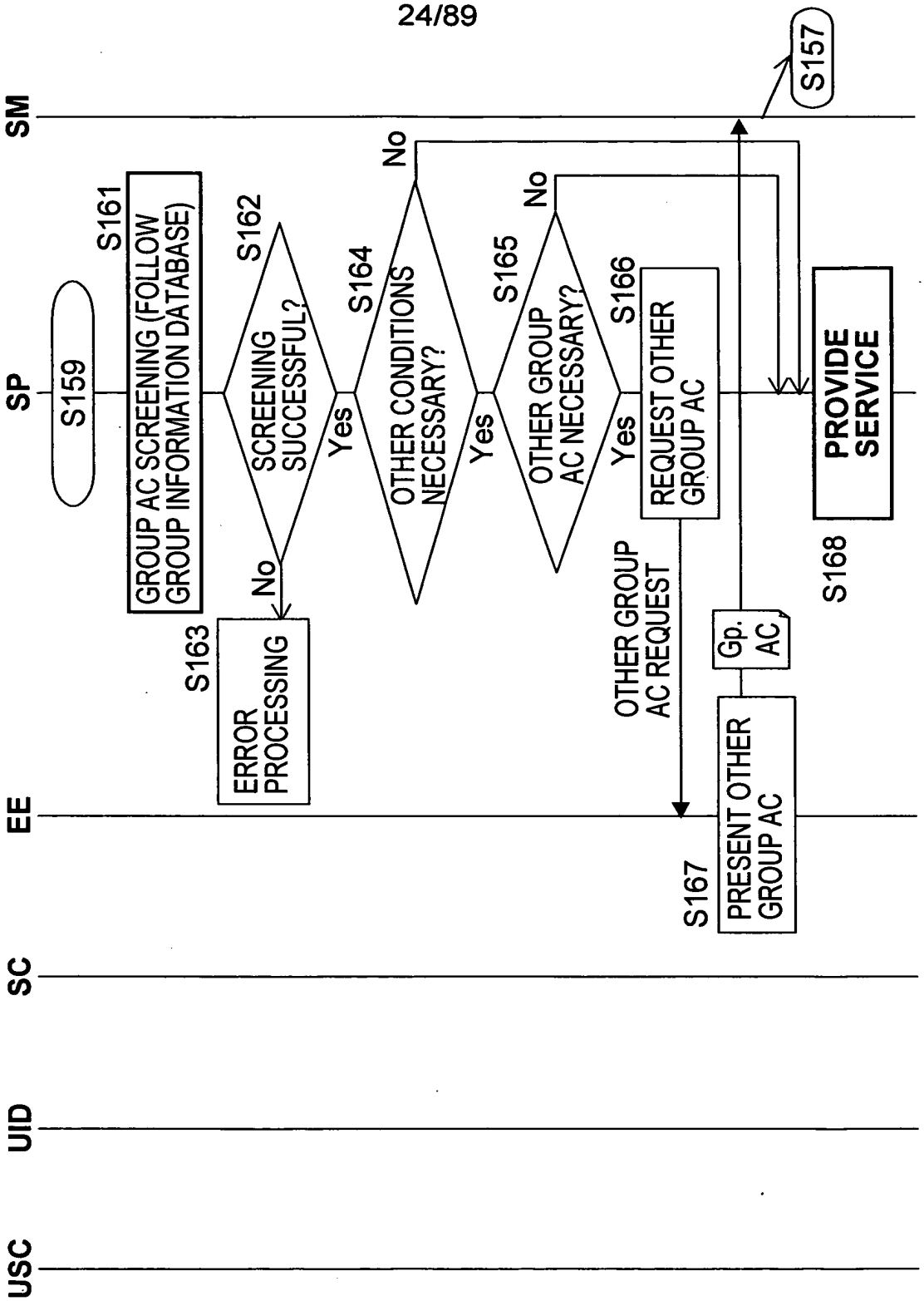

SM
SP
EE
SC
UID
USC
S157
S159
S161
GROUP AC SCREENING (FOLLOW GROUP INFORMATION DATABASE)
S162
SCREENING SUCCESSFUL?
Yes
No
S163
ERROR PROCESSING
S164
OTHER CONDITIONS NECESSARY?
Yes
No
S165
OTHER GROUP AC NECESSARY?
Yes
No
S166
REQUEST OTHER GROUP AC
OTHER GROUP AC REQUEST
S167
PRESENT OTHER GROUP AC
Gp. AC
S168
PROVIDE SERVICE

FIG. 24

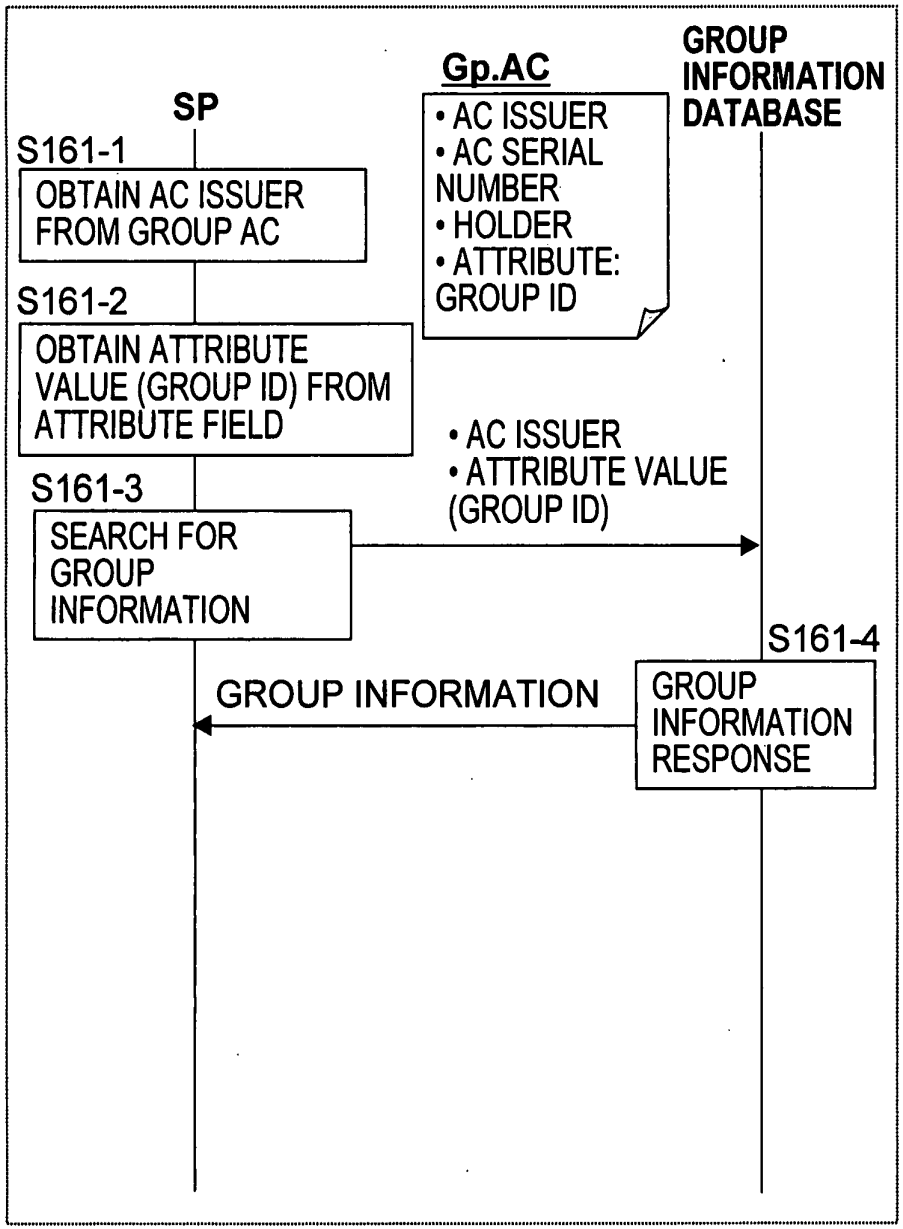


FIG. 25

EXAMPLE OF GROUP INFORMATION DATABASE

ISSUER	GROUP ID	GROUP INFORMATION
MANUFACTURER	1001	MAINTENANCE: FULL-SERVICE SUBSCRIBER
MANUFACTURER	1002	MAINTENANCE: TRIAL
GAME DISTRIBUTION SERVICE	1234-0	GAME DISTRIBUTION SERVICE MEMBER
GAME DISTRIBUTION SERVICE	1234-5-10	10-GAME USAGE MEMBER
TANAKA FAMILY, HEAD	001	TANAKA FAMILY, FAMILY
TANAKA FAMILY, HEAD	002	TANAKA FAMILY, CHILDREN

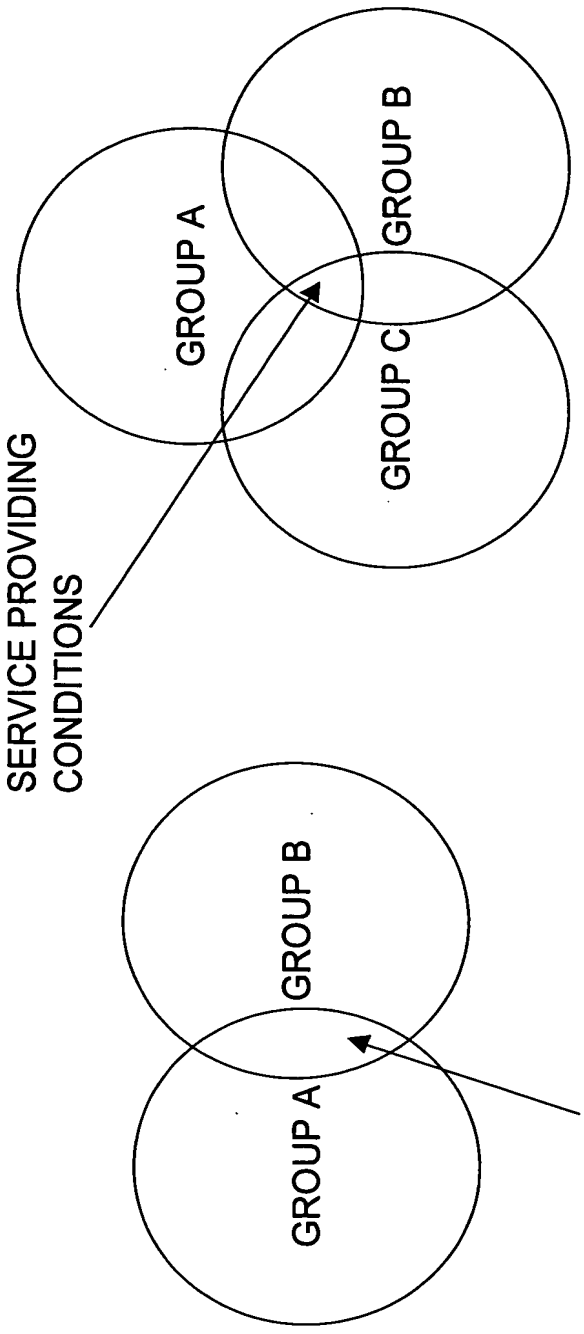

GROUP A
GROUP B
SERVICE PROVIDING CONDITIONS
(a)
GROUP A
GROUP B
GROUP C
SERVICE PROVIDING CONDITIONS
(b)

FIG. 26

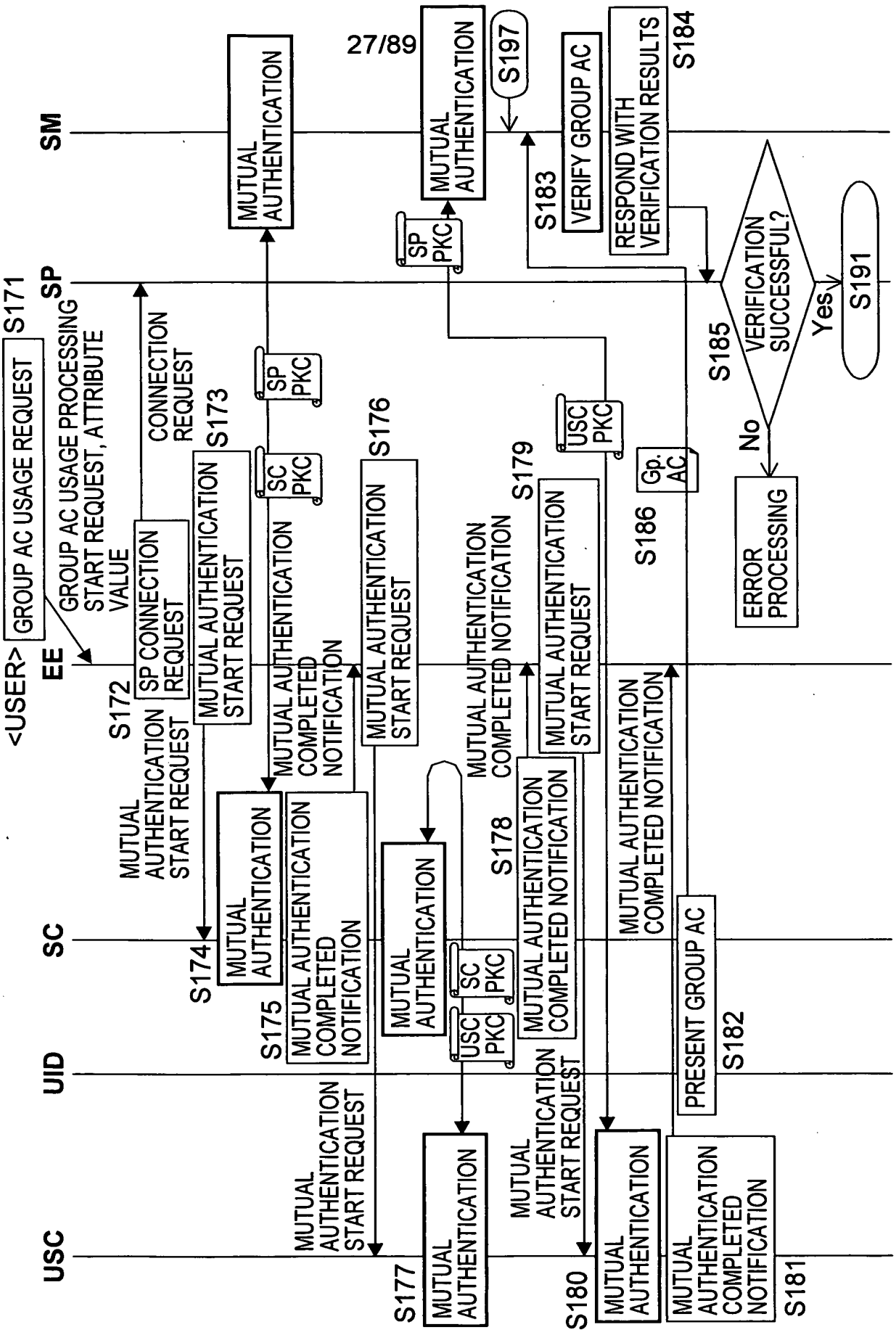

<USER>
EE
SP
SM
SC
UID
USC
GROUP AC USAGE REQUEST
S171
GROUP AC USAGE PROCESSING START REQUEST, ATTRIBUTE VALUE
SP CONNECTION REQUEST
S172
CONNECTION REQUEST
MUTUAL AUTHENTICATION START REQUEST
S173
MUTUAL AUTHENTICATION
SP PKC
SC PKC
MUTUAL AUTHENTICATION COMPLETED NOTIFICATION
S174
MUTUAL AUTHENTICATION
S175
MUTUAL AUTHENTICATION COMPLETED NOTIFICATION
MUTUAL AUTHENTICATION START REQUEST
S176
MUTUAL AUTHENTICATION
S177
USC PKC
S178
MUTUAL AUTHENTICATION COMPLETED NOTIFICATION
MUTUAL AUTHENTICATION START REQUEST
S179
MUTUAL AUTHENTICATION
S180
USC PKC
Gp. AC
S186
MUTUAL AUTHENTICATION COMPLETED NOTIFICATION
S181
PRESENT GROUP AC
S182
RESPOND WITH VERIFICATION RESULTS
S184
VERIFY GROUP AC
S183
MUTUAL AUTHENTICATION
S197
MUTUAL AUTHENTICATION
SP PKC
VERIFICATION SUCCESSFUL?
S185
Yes
S191
No
ERROR PROCESSING

FIG. 27

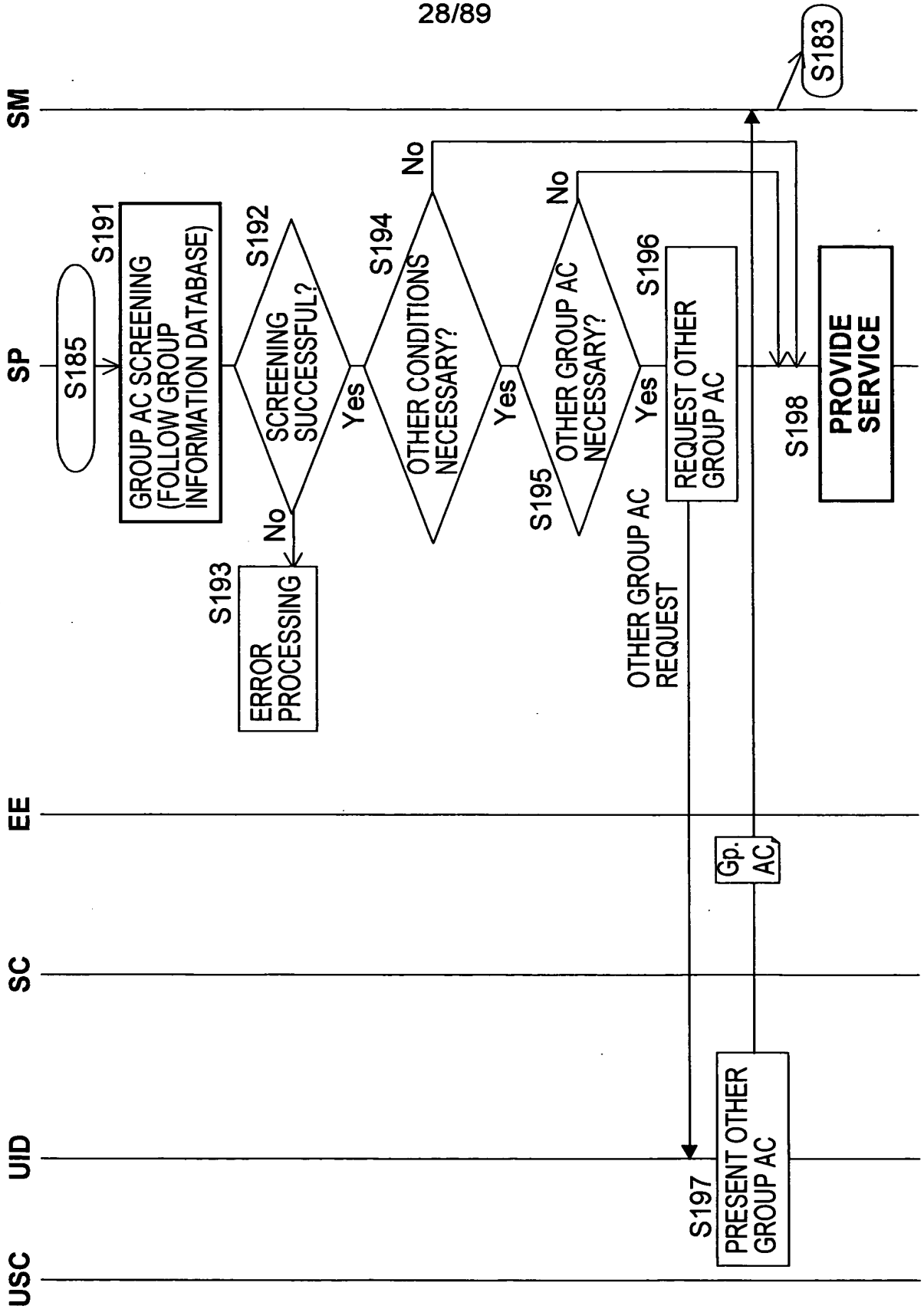

SM
SP
EE
SC
UID
USC
S183
S185
S191
GROUP AC SCREENING (FOLLOW GROUP INFORMATION DATABASE)
S192
SCREENING SUCCESSFUL?
No
Yes
S193
ERROR PROCESSING
S194
OTHER CONDITIONS NECESSARY?
No
Yes
S195
OTHER GROUP AC NECESSARY?
No
Yes
S196
REQUEST OTHER GROUP AC
OTHER GROUP AC REQUEST
S197
PRESENT OTHER GROUP AC
Gp. AC
S198
PROVIDE SERVICE

FIG. 28

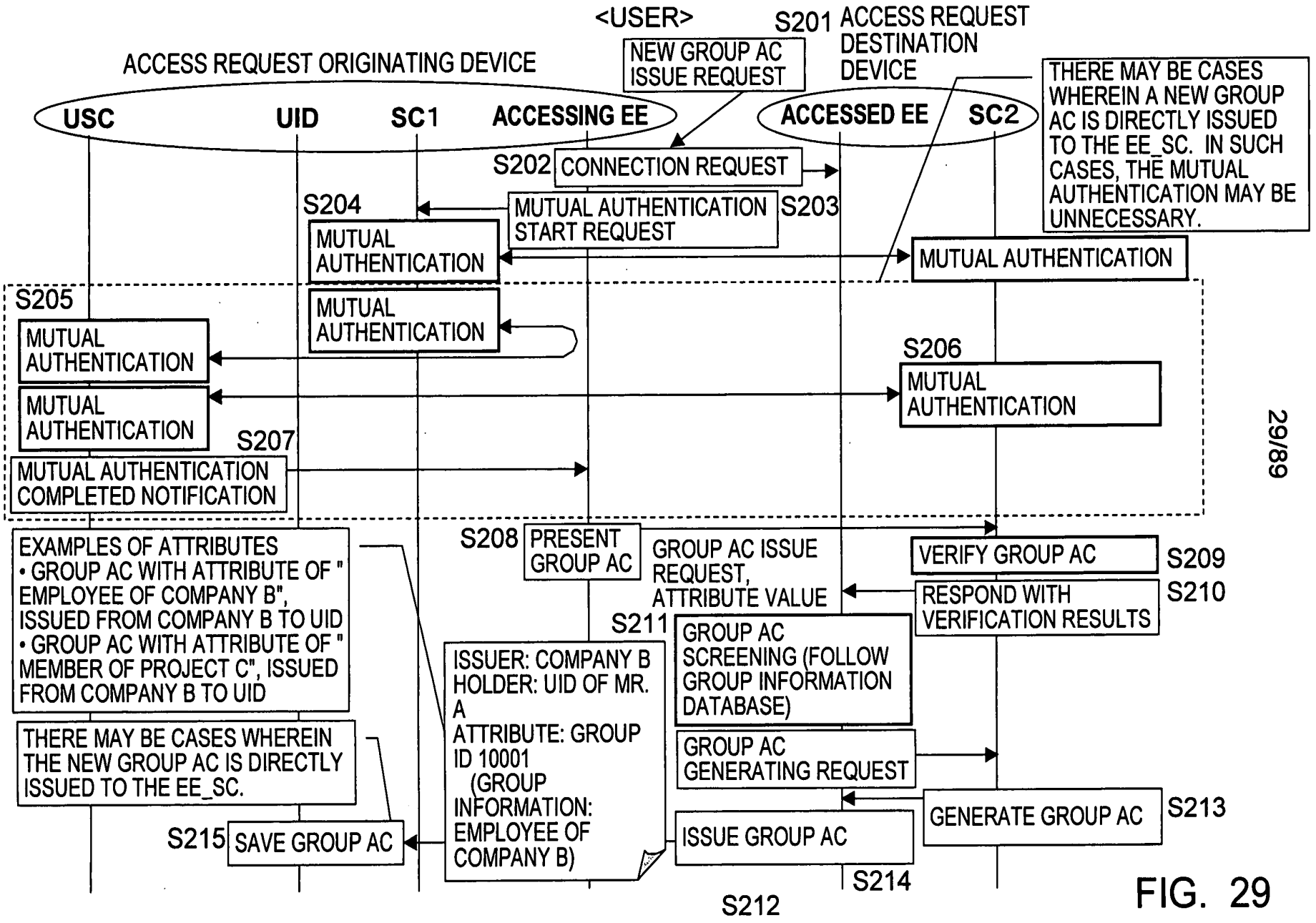


FIG. 29

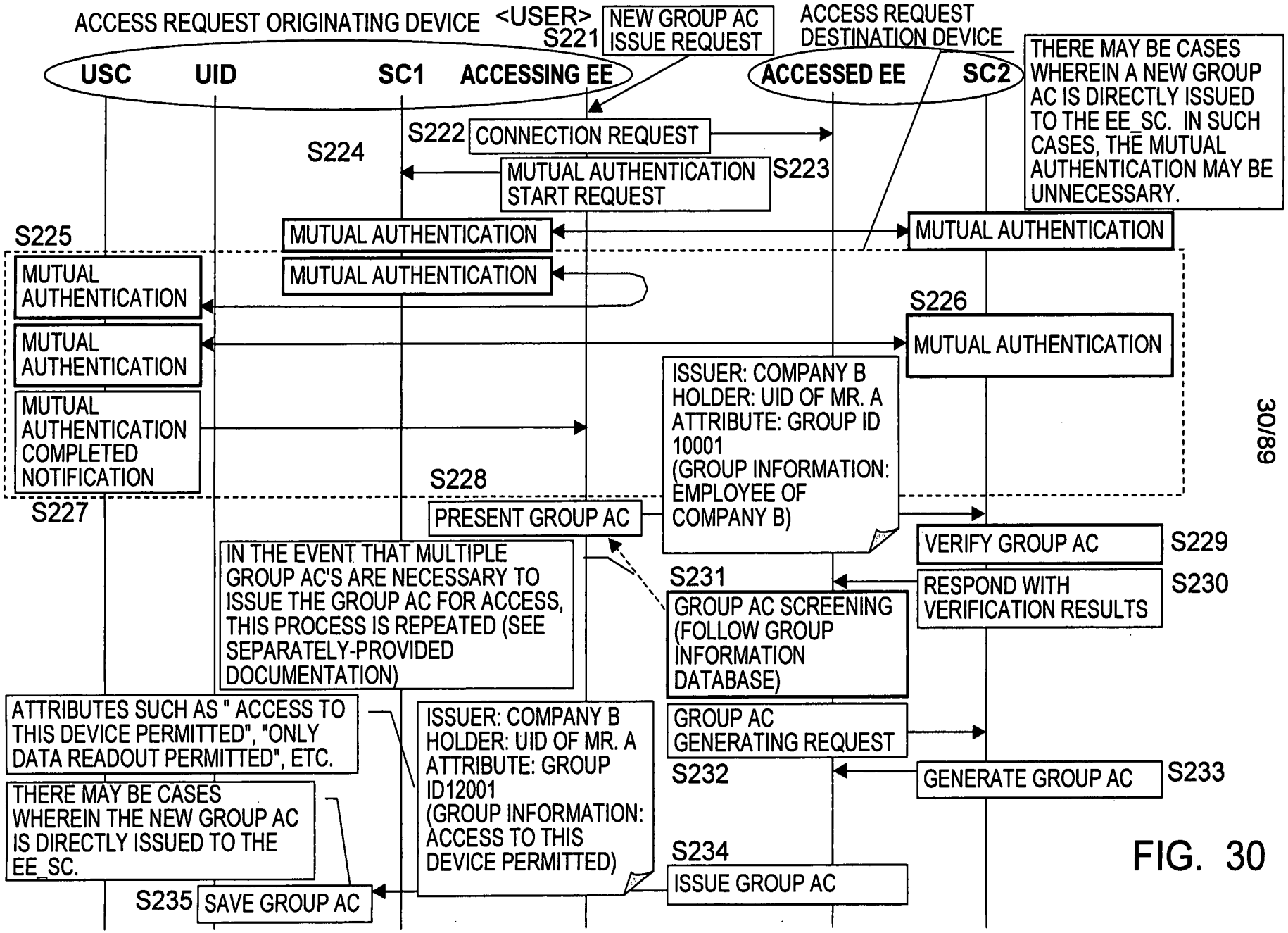
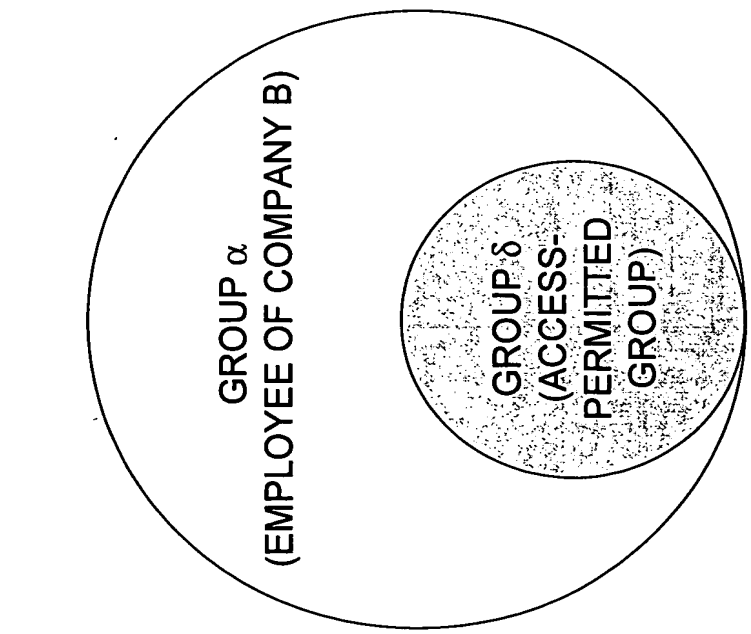


FIG. 30


GROUP α
(EMPLOYEE OF COMPANY B)
GROUP δ
(ACCESS-PERMITTED GROUP)
(a)

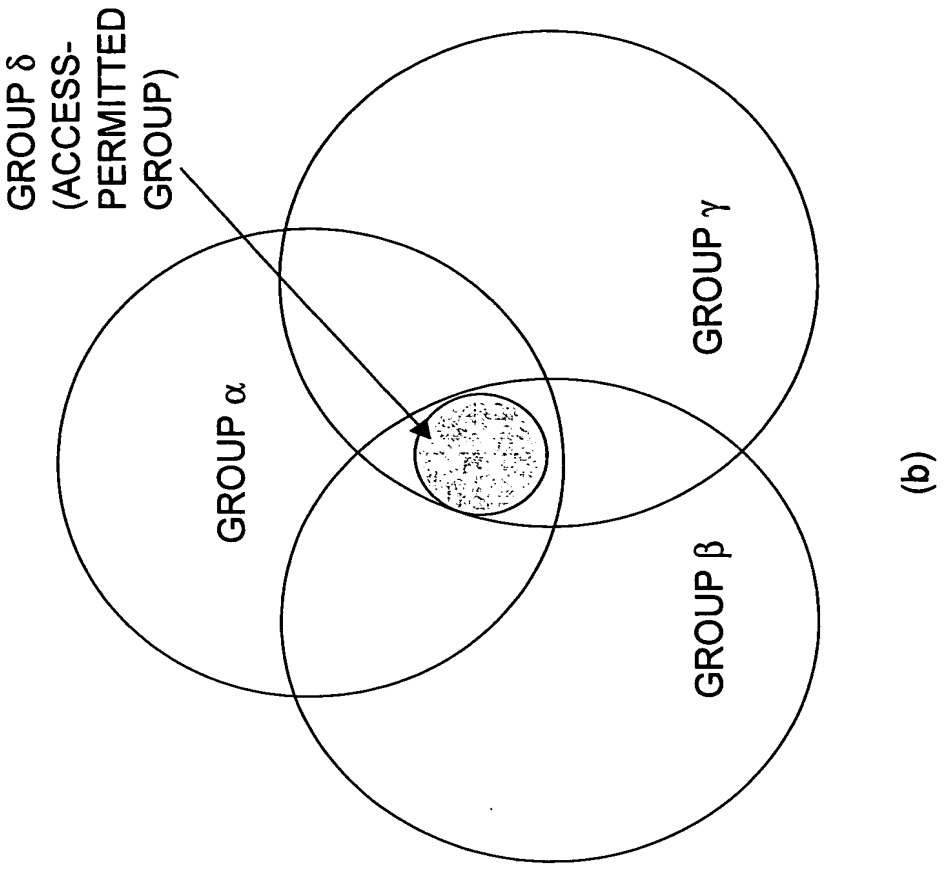
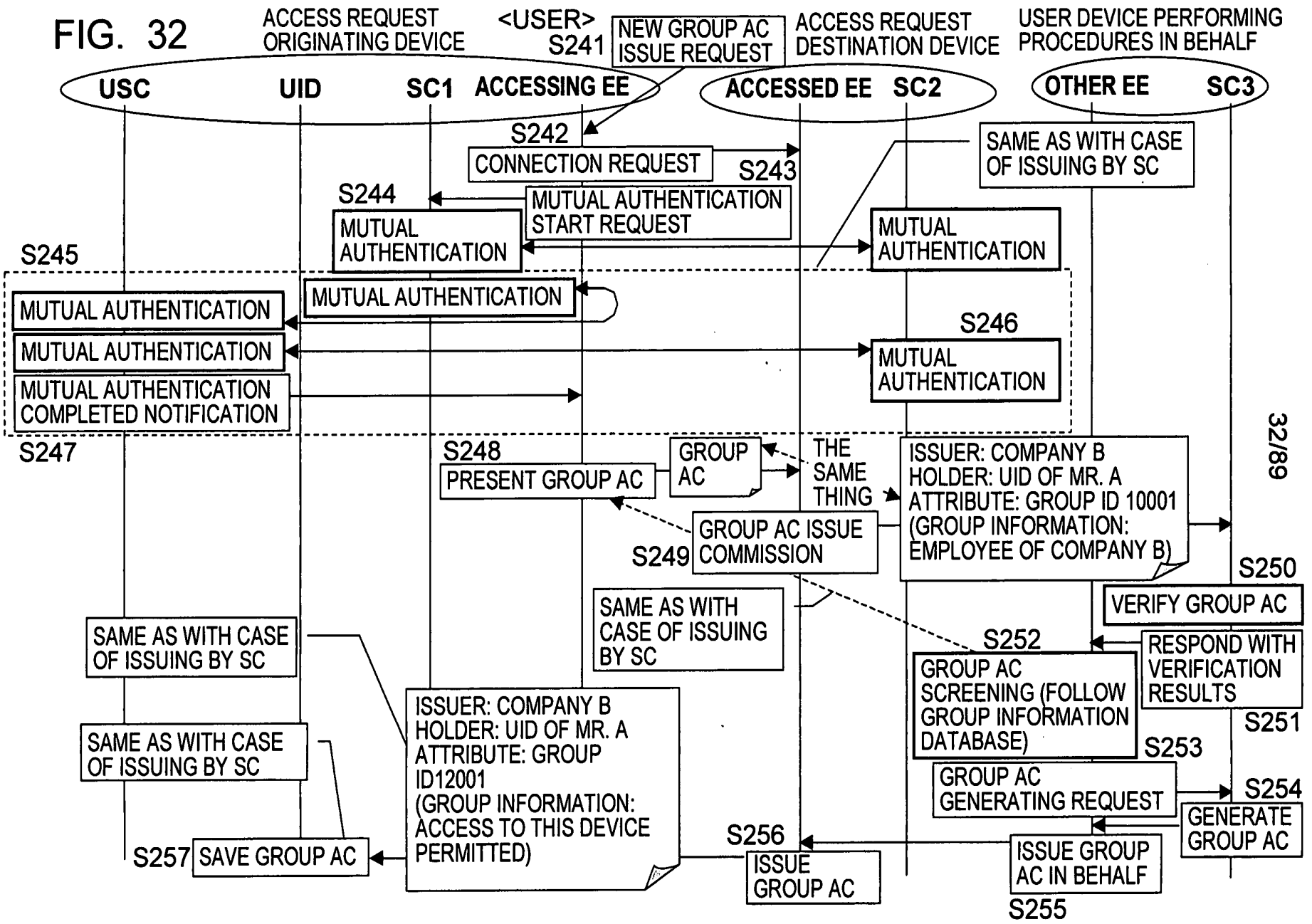

GROUP δ
(ACCESS-PERMITTED GROUP)
GROUP α
GROUP γ
GROUP β
(b)

FIG. 31

FIG. 32



32/89

10/517068

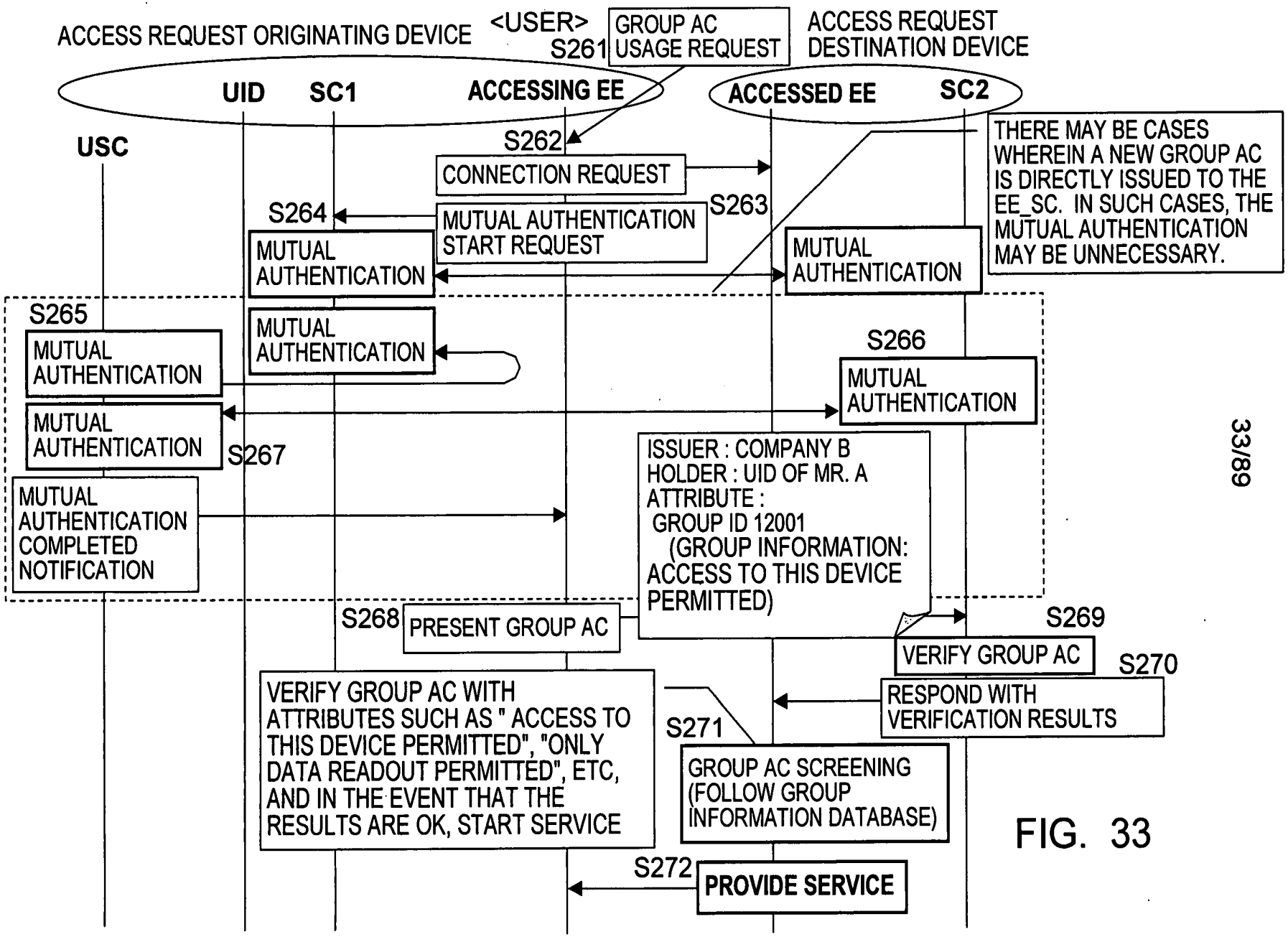


FIG. 33

ISSUER	ISSUING TIMING	HOLDER	VERIFIER	ATTRIBUTE
CARD COMPANY A	OPTIONAL (PERMISSIBLE EVEN BEFORE PURCHASING EE)	MR. A UID_USC	SP_SM	CARD COMPANY A MEMBER
COMPANY B	OPTIONAL (PERMISSIBLE EVEN BEFORE PURCHASING EE)	MR. A UID_USC	SP_SM	EMPLOYEE OF COMPANY B
CITY HALL	OPTIONAL (PERMISSIBLE EVEN BEFORE PURCHASING EE)	INDIVIDUAL FAMILY MEMBER UID_USC	SP_SM	FAMILY OF MR. A
MR. A	OPTIONAL (PERMISSIBLE EVEN BEFORE PURCHASING EE)	INDIVIDUAL FAMILY MEMBER UID_USC	SP_SM	FAMILY OF MR. A
EE MANUFACTURER C	AT TIME OF PURCHASING EE	MR. A UID_USC	SP_SM	USER REGISTRATION FOR EE
EE MANUFACTURER C	AT TIME OF MANUFACTURING EE	DEVICE EE_SC	SP_SM	EE REGISTRATION FOR EE
MR. A	AFTER PURCHASING EE	DEVICE EE_SC	SP_SM	OWNED BY ISSUER
EE MANUFACTURER C	AFTER PURCHASING EE	DEVICE EE_SC	SP_SM	DEVICE OF MR. A

FIG. 34

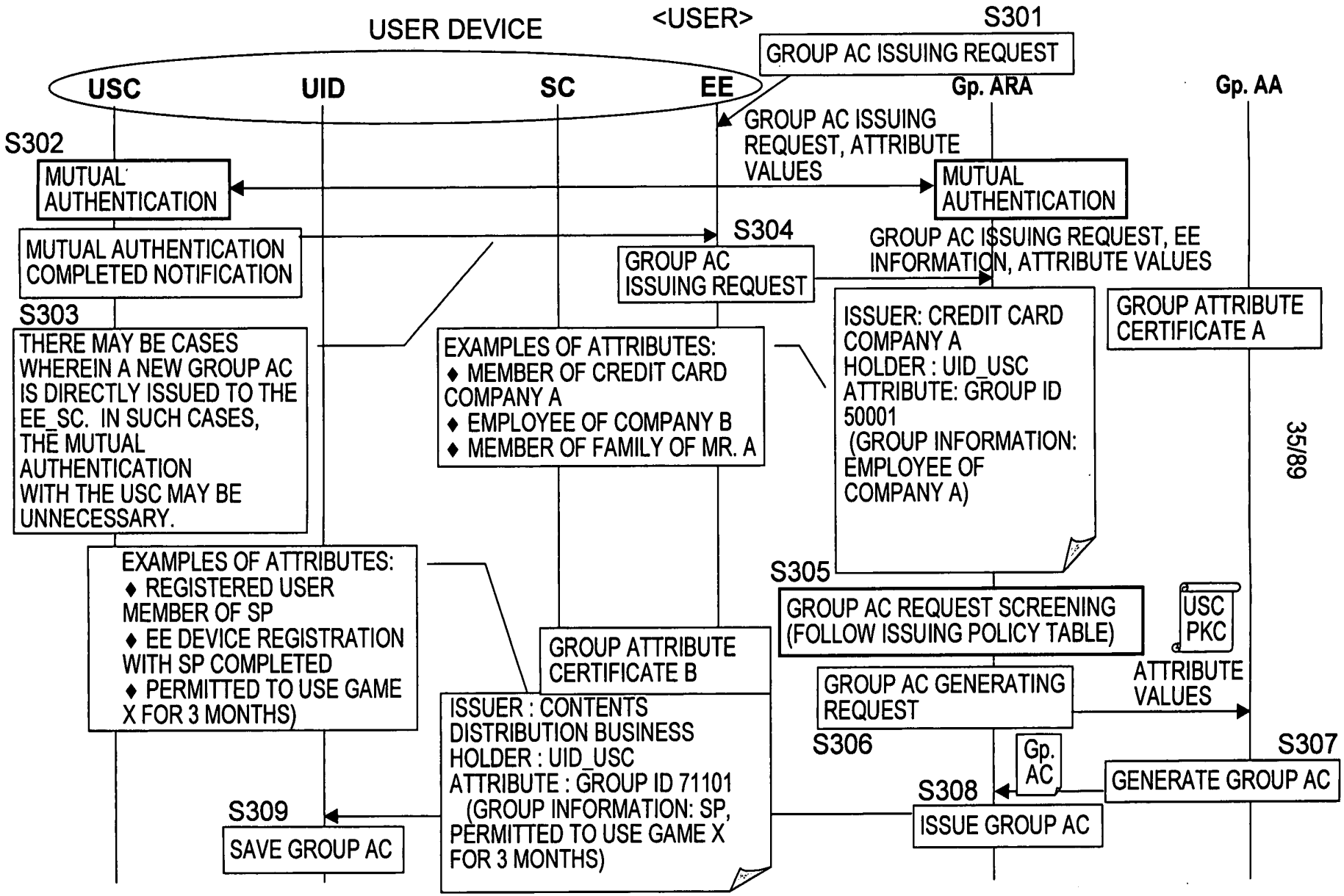


FIG. 35

10/517060

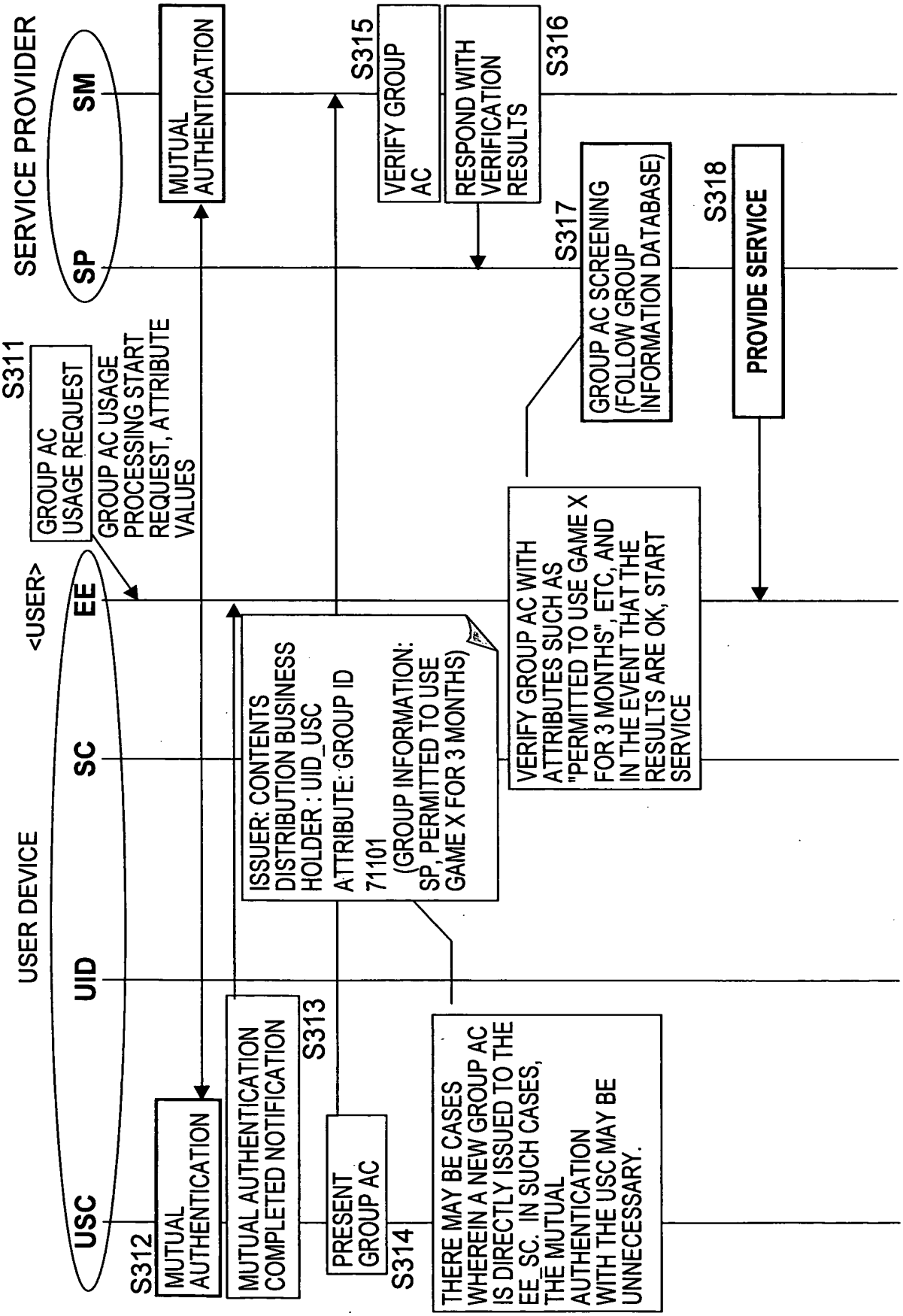

USER DEVICE
<USER>
SERVICE PROVIDER
USC
UID
SC
EE
SP
SM
S311
GROUP AC USAGE REQUEST
GROUP AC USAGE PROCESSING START REQUEST, ATTRIBUTE VALUES
MUTUAL AUTHENTICATION
S312
MUTUAL AUTHENTICATION
MUTUAL AUTHENTICATION COMPLETED NOTIFICATION
S313
ISSUER: CONTENTS DISTRIBUTION BUSINESS HOLDER : UID_USC
ATTRIBUTE: GROUP ID
71101
(GROUP INFORMATION: SP, PERMITTED TO USE GAME X FOR 3 MONTHS)
PRESENT GROUP AC
S314
THERE MAY BE CASES WHEREIN A NEW GROUP AC IS DIRECTLY ISSUED TO THE EE_SC. IN SUCH CASES, THE MUTUAL AUTHENTICATION WITH THE USC MAY BE UNNECESSARY.
S315
VERIFY GROUP AC
RESPOND WITH VERIFICATION RESULTS
S316
S317
GROUP AC SCREENING (FOLLOW GROUP INFORMATION DATABASE)
VERIFY GROUP AC WITH ATTRIBUTES SUCH AS "PERMITTED TO USE GAME X FOR 3 MONTHS", ETC, AND IN THE EVENT THAT THE RESULTS ARE OK, START SERVICE
S318
PROVIDE SERVICE

FIG. 36

	AC TITLE	ATTRIBUTE INFORMATION (= ISSUING POLICY)	ISSUER (GROUP AA, ARA)	HOLDER
AC01	1. STUDENT ID CARD	STUDENT OF ISSUER	UNIVERSITY A (AA OPERATED (MANAGED) THEREBY)	USC OF UID OF USER C
AC02	2. ART CLASS PARTICIPANT CARD	HOLDER OF RIGHT TO PARTICIPATE IN ART CLASSES HOSTED BY ISSUER	UNIVERSITY A (AA OPERATED (MANAGED) THEREBY)	USC OF UID OF USER C
AC03	3. MANAGED DEVICE CERTIFICATE	DEVICE MANAGED BY ISSUER	UNIVERSITY A (AA OPERATED (MANAGED) THEREBY)	SC OF TELEVISION D WHICH IS AN END ENTITY (EE)
AC04	4. EDUCATIONAL DEVICE CERTIFICATE	DEVICE FOR EDUCATIONAL USE	MINISTRY OF EDUCATION, CULTURE, SPORTS, SCIENCE AND TECHNOLOGY (AA OPERATED (MANAGED) THEREBY)	SC OF TELEVISION D WHICH IS AN END ENTITY (EE)

FIG. 37

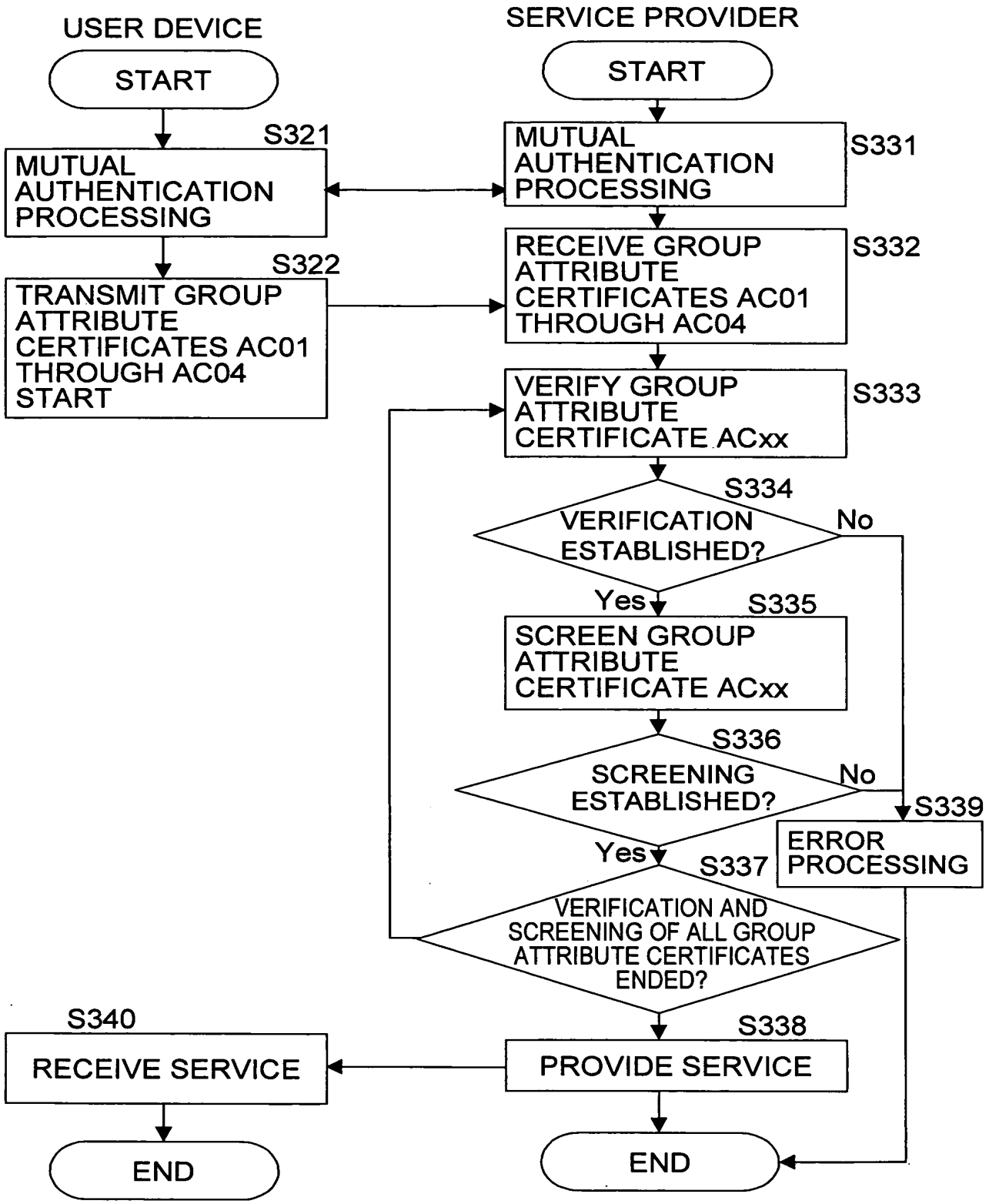

USER DEVICE
SERVICE PROVIDER
START
START
S321
MUTUAL AUTHENTICATION PROCESSING
MUTUAL AUTHENTICATION PROCESSING
S331
S322
TRANSMIT GROUP ATTRIBUTE CERTIFICATES AC01 THROUGH AC04 START
RECEIVE GROUP ATTRIBUTE CERTIFICATES AC01 THROUGH AC04
S332
VERIFY GROUP ATTRIBUTE CERTIFICATE ACxx
S333
S334
VERIFICATION ESTABLISHED?
No
Yes
S335
SCREEN GROUP ATTRIBUTE CERTIFICATE ACxx
S336
SCREENING ESTABLISHED?
No
S339
ERROR PROCESSING
Yes
S337
VERIFICATION AND SCREENING OF ALL GROUP ATTRIBUTE CERTIFICATES ENDED?
S340
S338
RECEIVE SERVICE
PROVIDE SERVICE
END
END

FIG. 38

SERVICE	AC ISSUER, AC	. . .	AC ISSUER, AC	INFORMATION OTHER THAN AC	. . .
VIEW/LISTEN CONTENTS B	UNIVERSITY A, STUDENT IDENTIFICATION CARD		MINISTRY OF EDUCATION, CULTURE, SPORTS, SCIENCE AND TECHNOLOGY, EDUCATIONAL DEVICE CERTIFICATE		
VIEW/LISTEN CONTENTS B					
. . .					
VIEW/LISTEN CONTENTS G					

FIG. 39

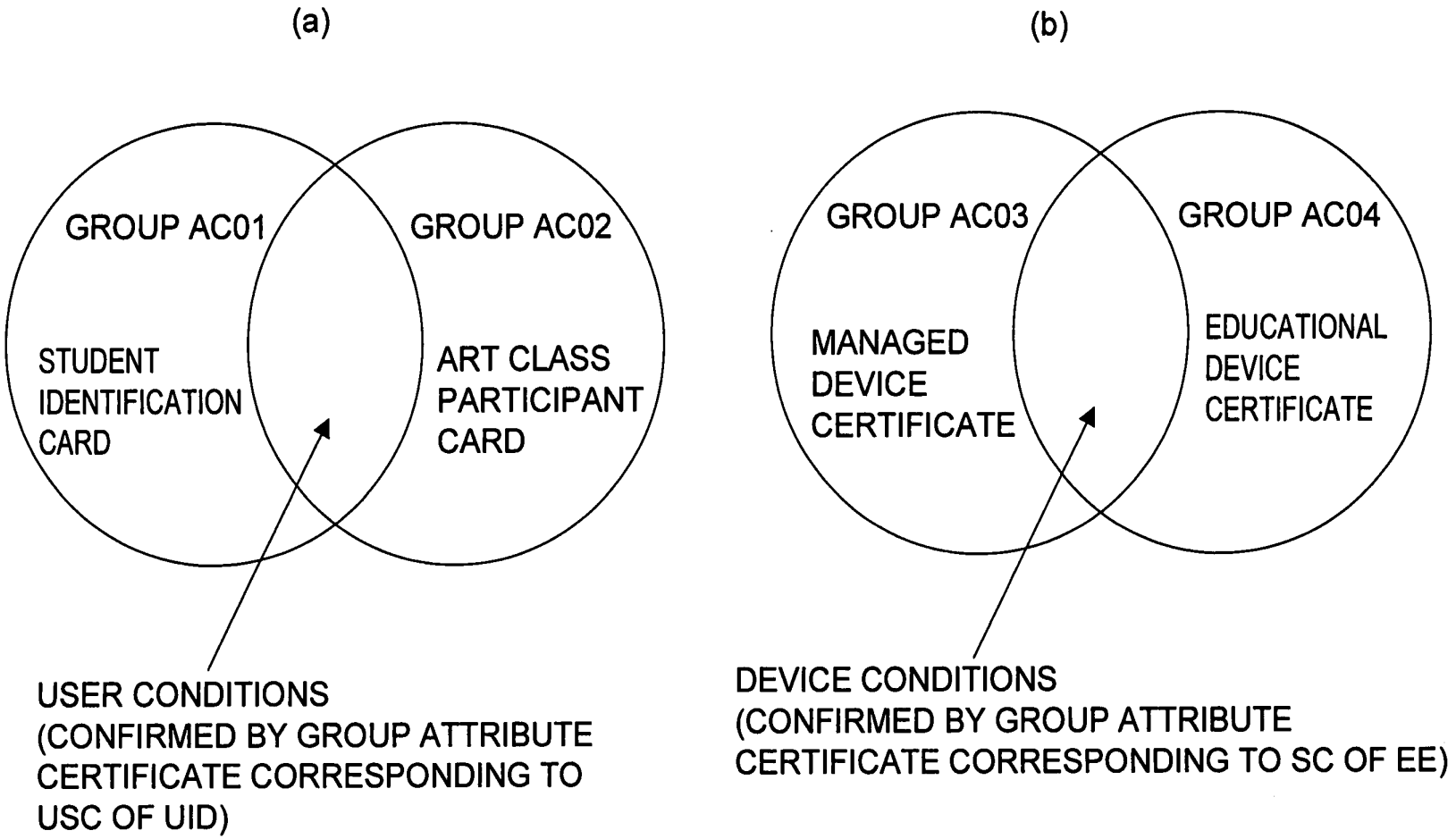


FIG. 40

	ISSUER	HOLDER	VERIFIER	ATTRIBUTE
AC01	HOSPITAL SIDE MEDICAL DEVICE (SP)	UID_USC OR EE_SC OF MR. A	HOSPITAL SIDE MEDICAL DEVICE (SP_SM)	PERMITTED TO RUN PROGRAM E
AC02	HOME SIDE MEDICAL DEVICE (EE)	HOSPITAL SIDE MEDICAL DEVICE (SP_SM)	HOME SIDE MEDICAL DEVICE (EE_SC)	PERMITTED TO HANDLE DATA X

FIG. 41

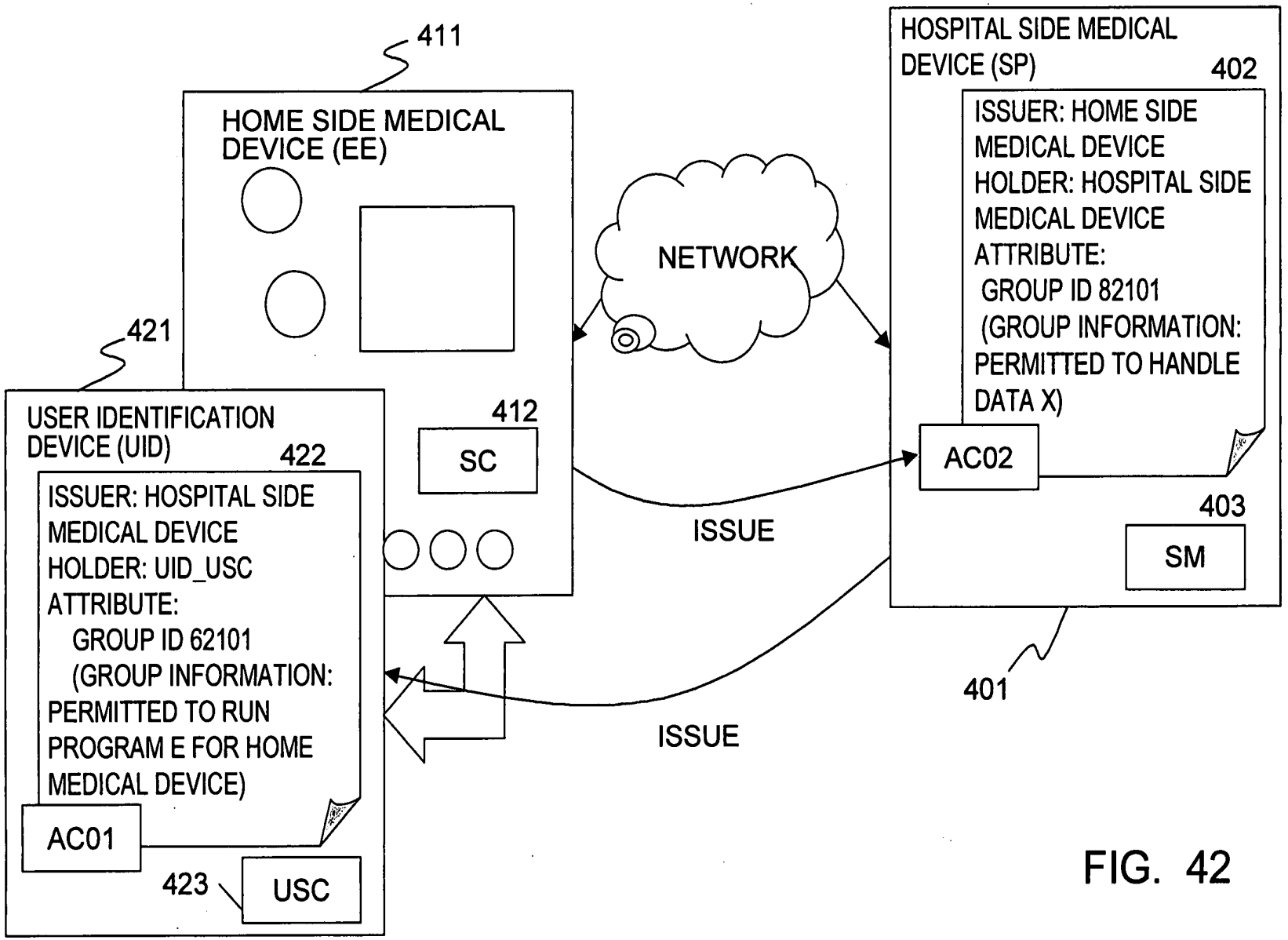


FIG. 42

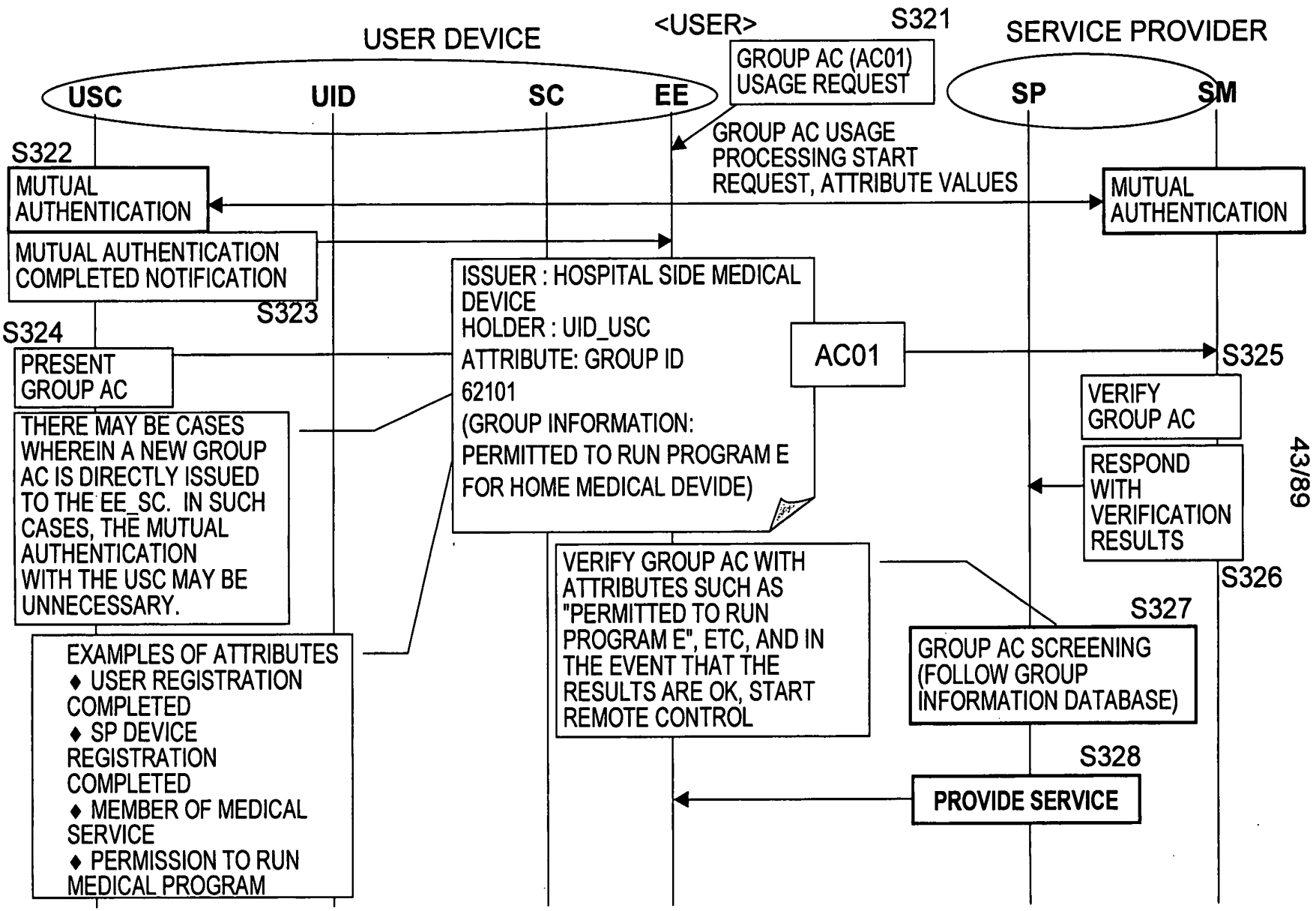


FIG. 43

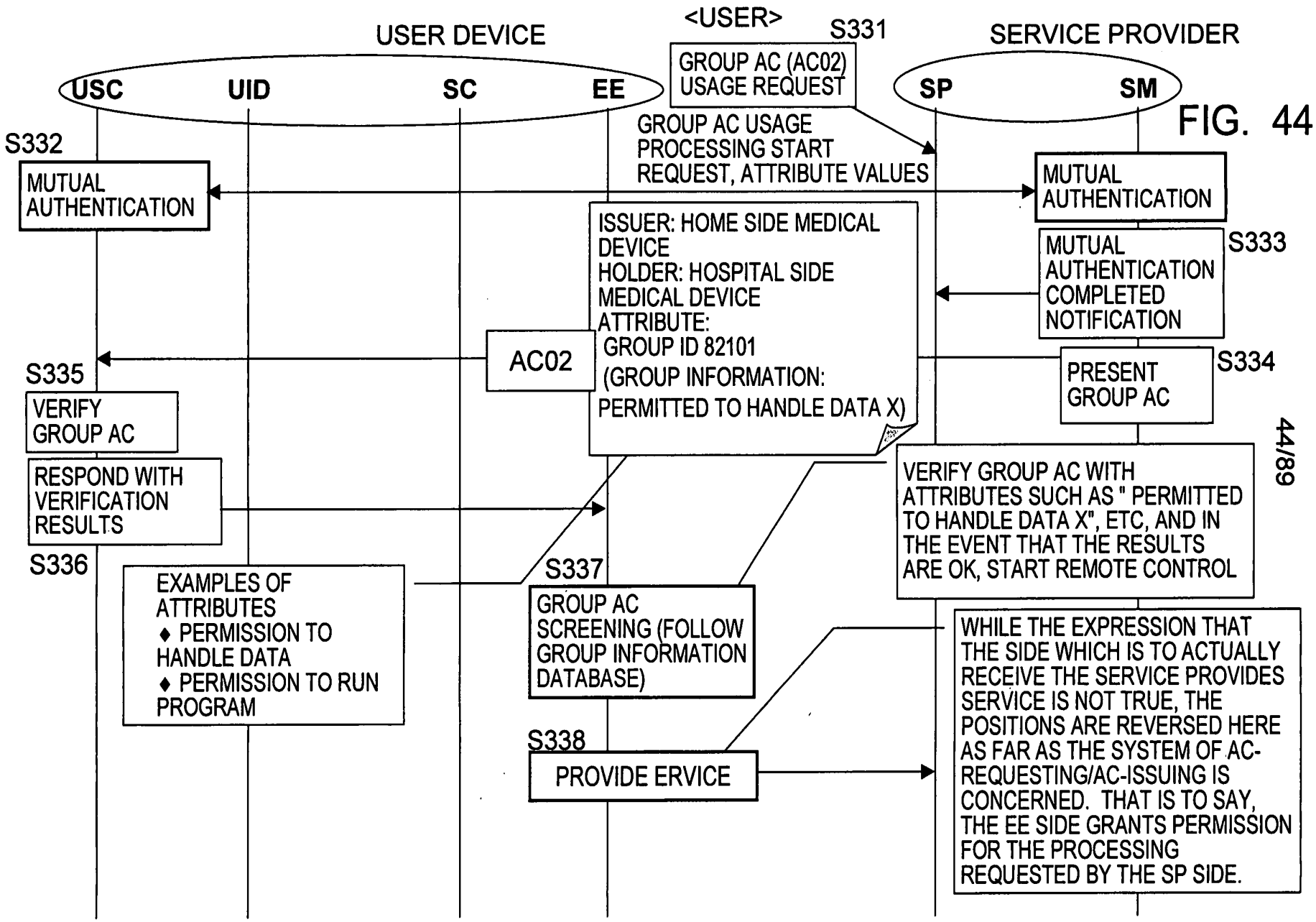


FIG. 44

	ISSUER	ISSUING TIMING	HOLDER	VERIFIER	ATTRIBUTE
SERVICE AC	HOME APPLIANCE MANUFACTURER (SP)	AT TIME OF PURCHASING HOME APPLIANCE	MR. A UID_USC or EE_SC	SP_SM	EE MAINTENANCE SERVICE CONTENTS
CONTROL AC	HOME APPLIANCE (EE)	PRIOR TO OR AT TIME OF AUTOMATIC MAINTENANCE	SP_SM	EE_SC	HOME APPLIANCE CONTROL CONSTRAINT RANGE X

FIG. 45

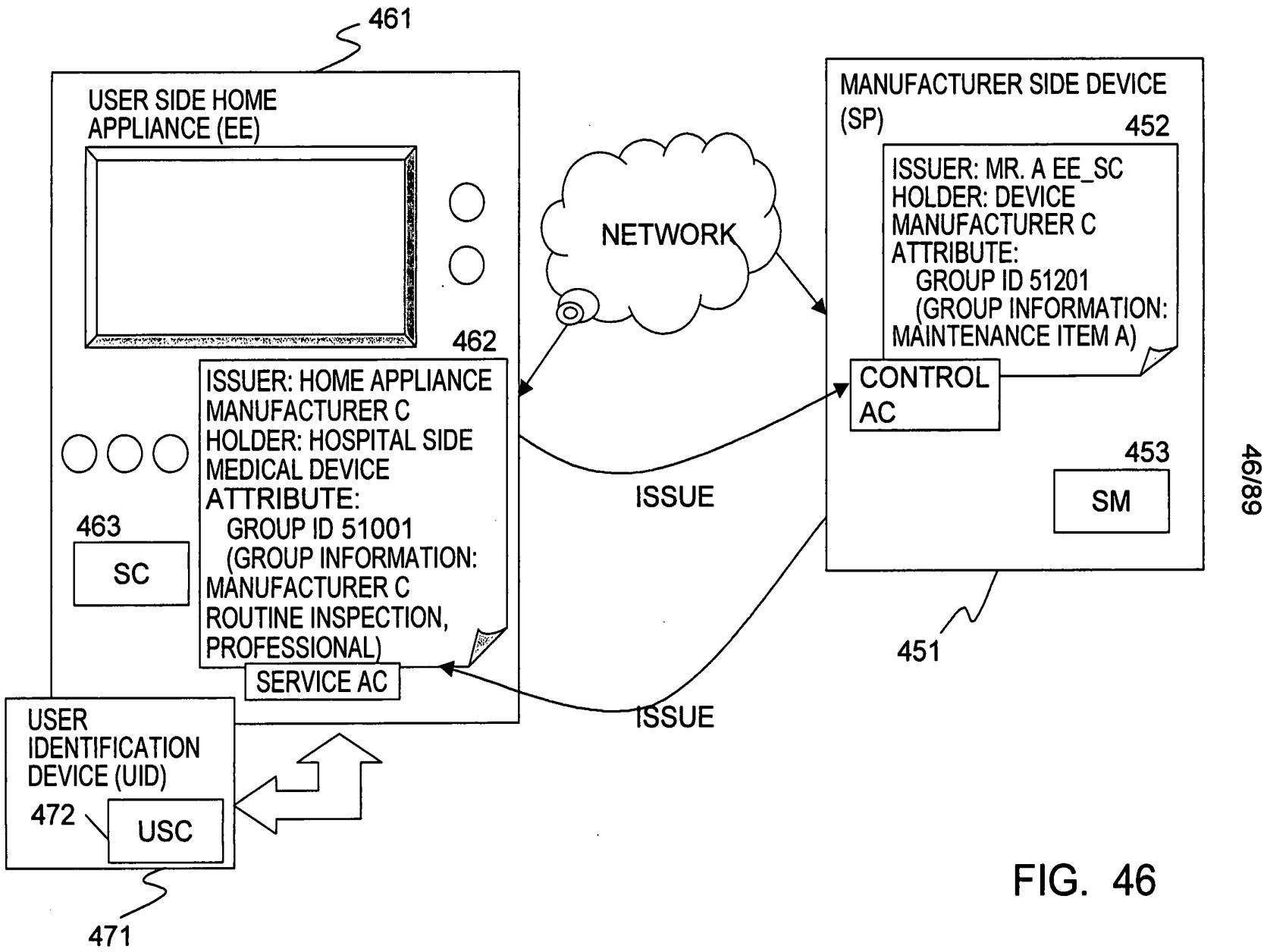


FIG. 46

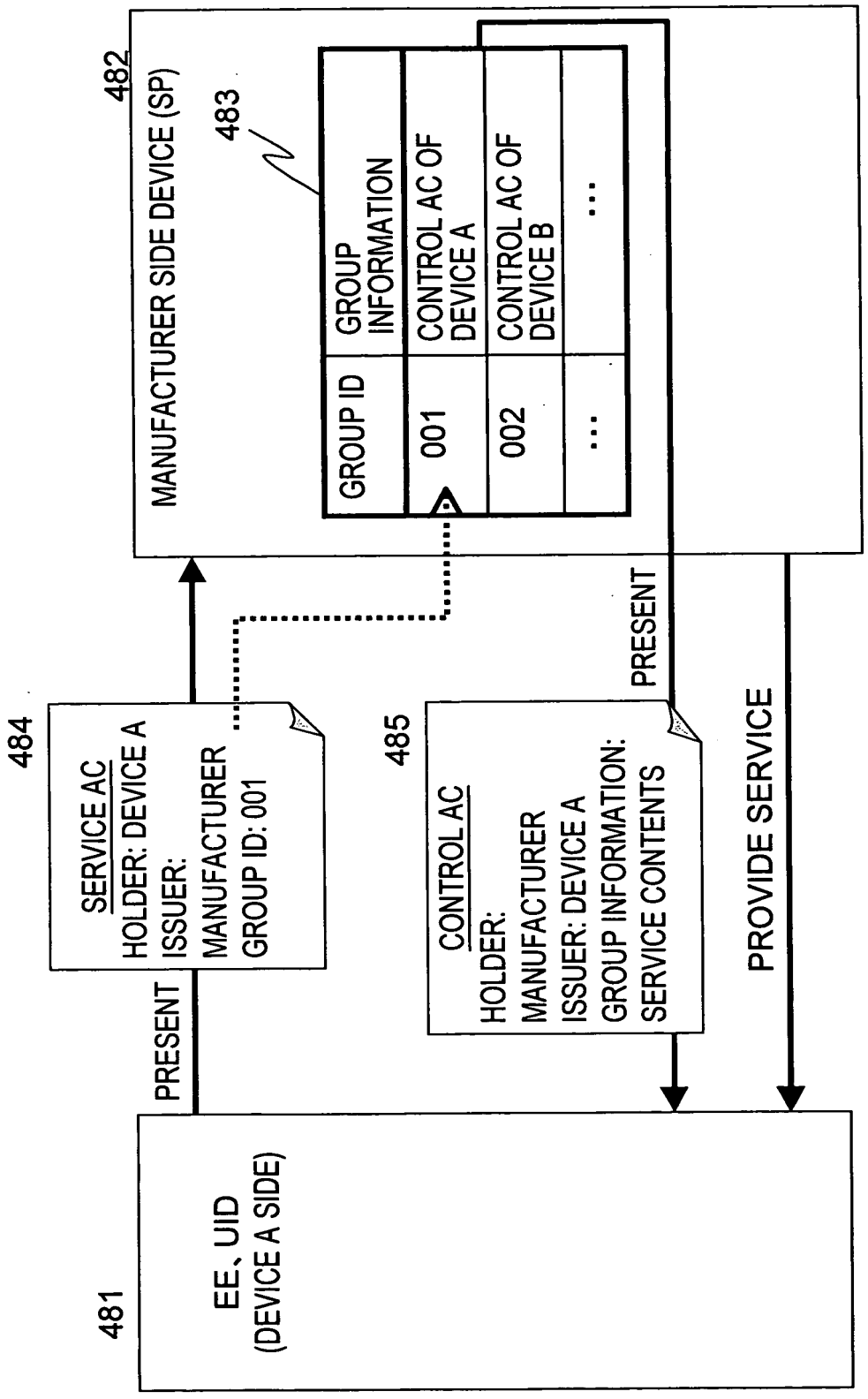

481
EE, UID
(DEVICE A SIDE)
482
MANUFACTURER SIDE DEVICE (SP)
483
GROUP ID
GROUP INFORMATION
001
CONTROL AC OF DEVICE A
002
CONTROL AC OF DEVICE B
...
...
484
SERVICE AC
HOLDER: DEVICE A
ISSUER: MANUFACTURER
GROUP ID: 001
485
CONTROL AC
HOLDER: MANUFACTURER
ISSUER: DEVICE A
GROUP INFORMATION: SERVICE CONTENTS
PRESENT
PRESENT
PROVIDE SERVICE

FIG. 47

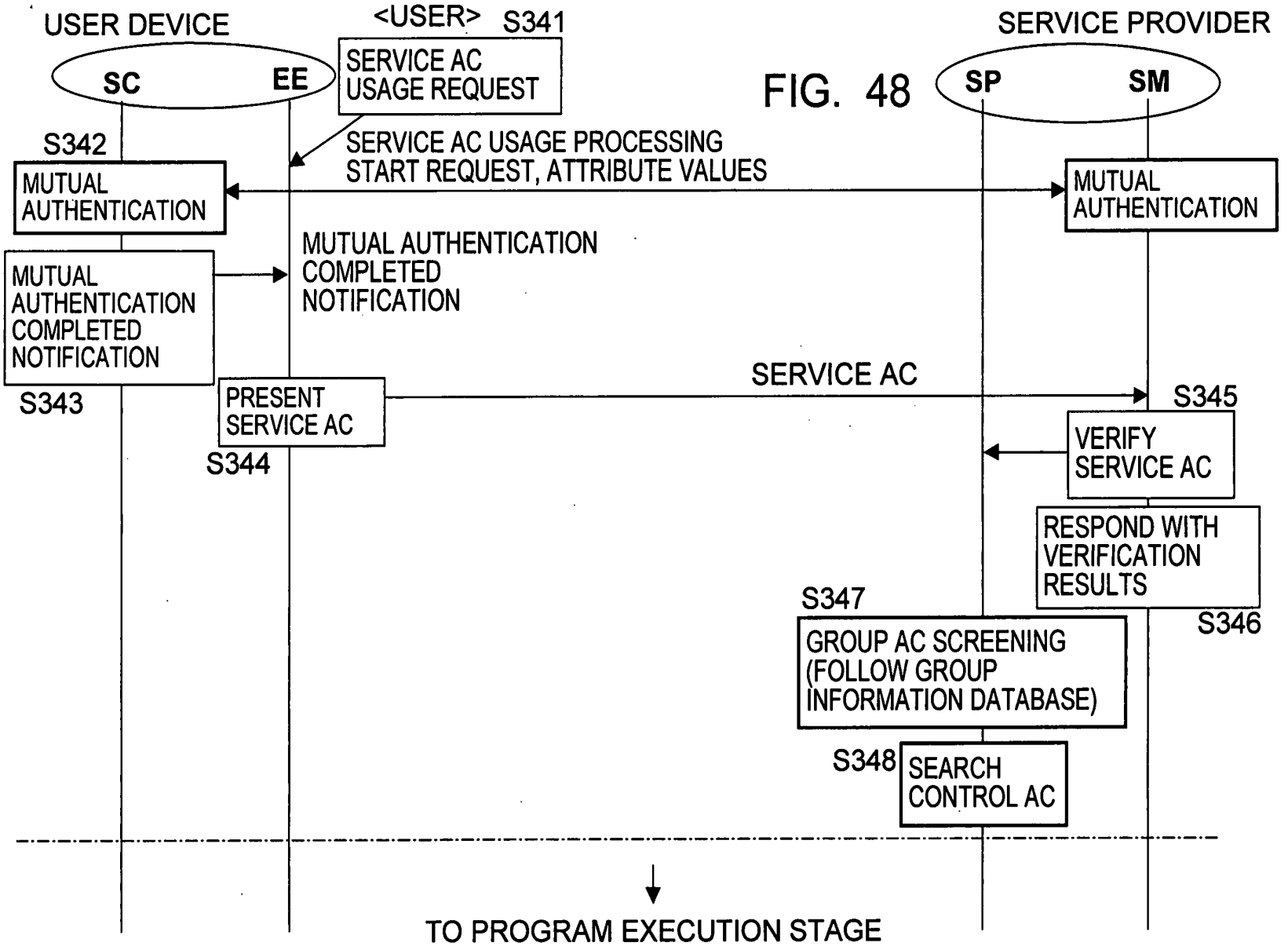
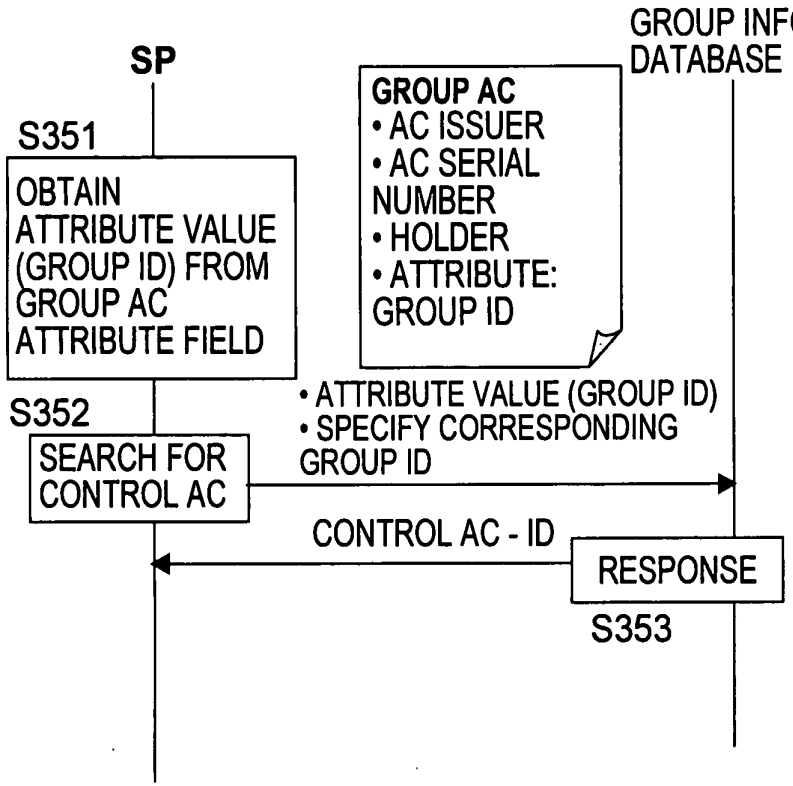


FIG. 48

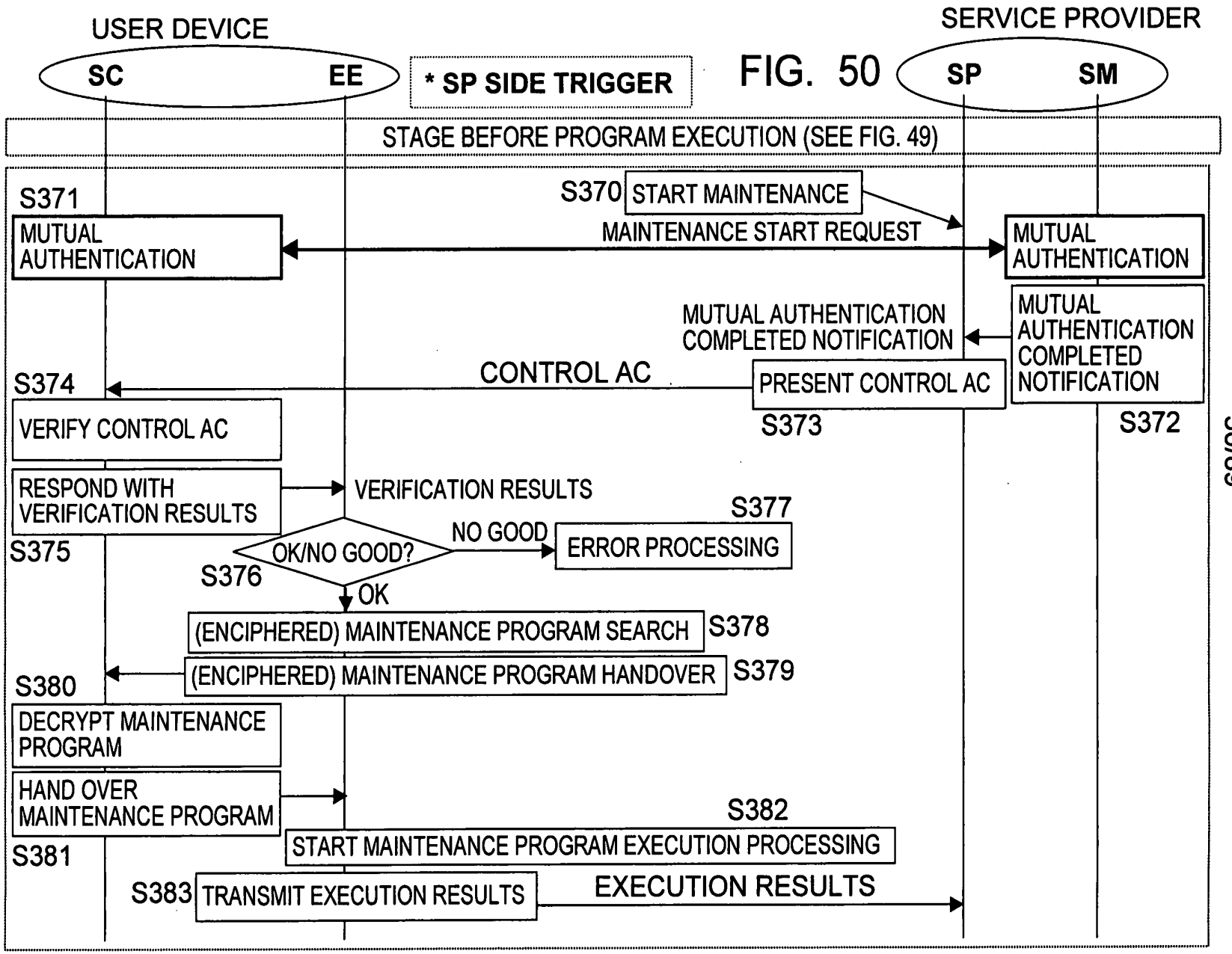


EXAMPLES OF GROUP INFORMATION (CONTROL AC) DATABASE

ISSUER	GROUP ID (SERVICE AC)	GROUP INFORMATION (CORRESPONDING CONTROL AC ID)
MR. A EE_SC	51001 ROUTINE INSPECTION, PROFESSIONAL	51202 MAINTENANCE ITEM A
MR. A EE_SC	51001 ROUTINE INSPECTION, PROFESSIONAL	51202 MAINTENANCE ITEM B
MR. A EE_SC	51001 ROUTINE INSPECTION, PROFESSIONAL	51202 MAINTENANCE ITEM C

ISSUER	GROUP ID (SERVICE AC)	GROUP INFORMATION (CORRESPONDING CONTROL AC ID)
MR. A EE_SC	51002 ROUTINE INSPECTION, ECONOMY	51201 MAINTENANCE ITEM A
MR. A EE_SC	51002 ROUTINE INSPECTION, ECONOMY	51204 MAINTENANCE ITEM D

FIG. 49


USER DEVICE
SC
EE
* SP SIDE TRIGGER
SERVICE PROVIDER
SP
SM
FIG. 50
STAGE BEFORE PROGRAM EXECUTION (SEE FIG. 49)
S370
START MAINTENANCE
MAINTENANCE START REQUEST
S371
MUTUAL AUTHENTICATION
MUTUAL AUTHENTICATION
MUTUAL AUTHENTICATION COMPLETED NOTIFICATION
MUTUAL AUTHENTICATION COMPLETED NOTIFICATION
S372
CONTROL AC
PRESENT CONTROL AC
S373
S374
VERIFY CONTROL AC
RESPOND WITH VERIFICATION RESULTS
VERIFICATION RESULTS
S375
OK/NO GOOD?
S376
NO GOOD
S377
ERROR PROCESSING
OK
(ENCIPHERED) MAINTENANCE PROGRAM SEARCH
S378
(ENCIPHERED) MAINTENANCE PROGRAM HANDOVER
S379
S380
DECRYPT MAINTENANCE PROGRAM
HAND OVER MAINTENANCE PROGRAM
S381
S382
START MAINTENANCE PROGRAM EXECUTION PROCESSING
S383
TRANSMIT EXECUTION RESULTS
EXECUTION RESULTS

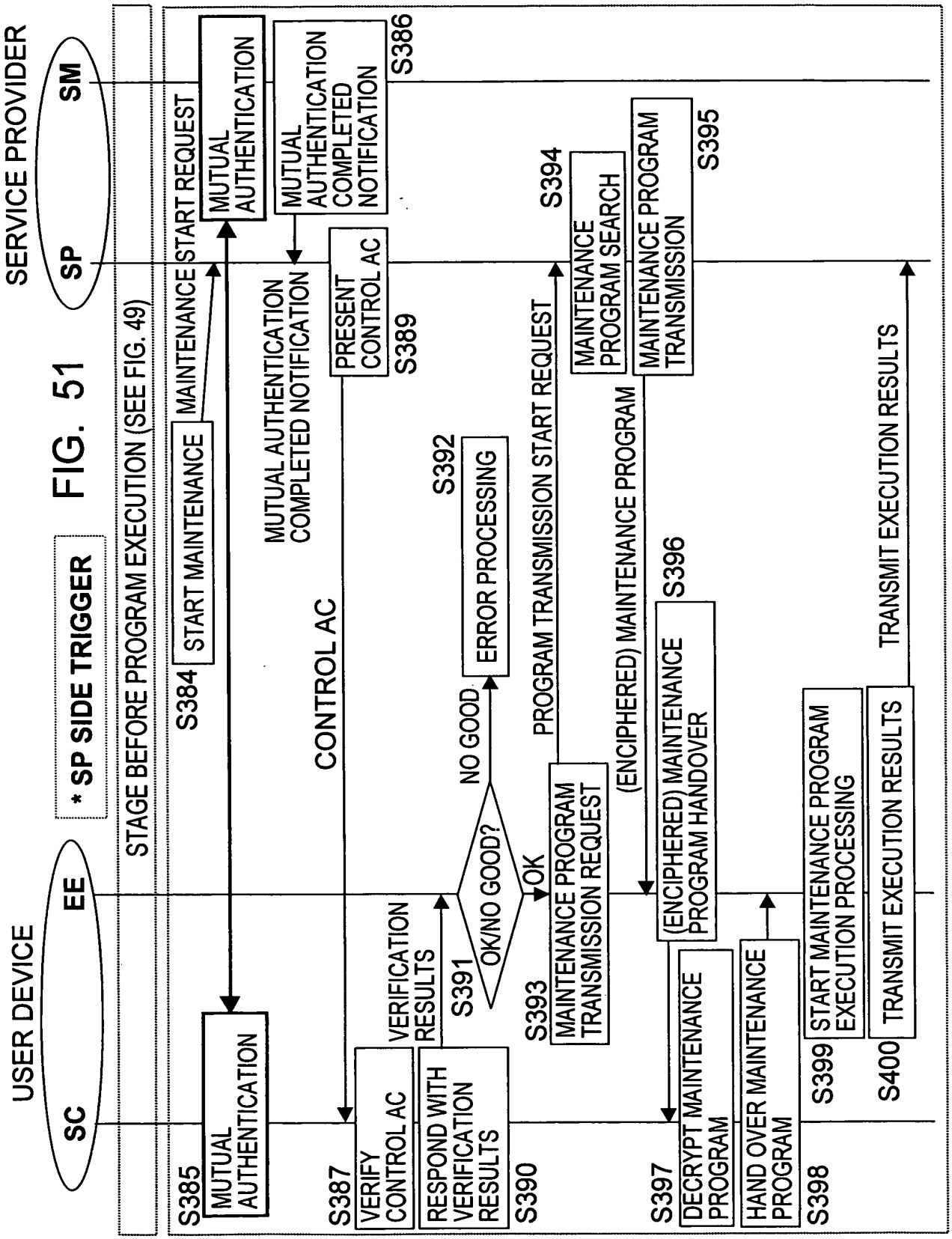

USER DEVICE
SC
EE
SERVICE PROVIDER
SP
SM
* SP SIDE TRIGGER
STAGE BEFORE PROGRAM EXECUTION (SEE FIG. 49)
S384
START MAINTENANCE
MAINTENANCE START REQUEST
MUTUAL AUTHENTICATION
MUTUAL AUTHENTICATION COMPLETED NOTIFICATION
S386
S385
MUTUAL AUTHENTICATION
MUTUAL AUTHENTICATION COMPLETED NOTIFICATION
PRESENT CONTROL AC
S389
CONTROL AC
S387
VERIFY CONTROL AC
VERIFICATION RESULTS
RESPOND WITH VERIFICATION RESULTS
S390
S391
OK/NO GOOD?
NO GOOD
S392
ERROR PROCESSING
OK
S393
MAINTENANCE PROGRAM TRANSMISSION REQUEST
PROGRAM TRANSMISSION START REQUEST
S394
MAINTENANCE PROGRAM SEARCH
MAINTENANCE PROGRAM TRANSMISSION
S395
(ENCIPHERED) MAINTENANCE PROGRAM
S396
(ENCIPHERED) MAINTENANCE PROGRAM HANDOVER
S397
DECRYPT MAINTENANCE PROGRAM
HAND OVER MAINTENANCE PROGRAM
S398
S399
START MAINTENANCE PROGRAM EXECUTION PROCESSING
TRANSMIT EXECUTION RESULTS
S400
TRANSMIT EXECUTION RESULTS

FIG. 51

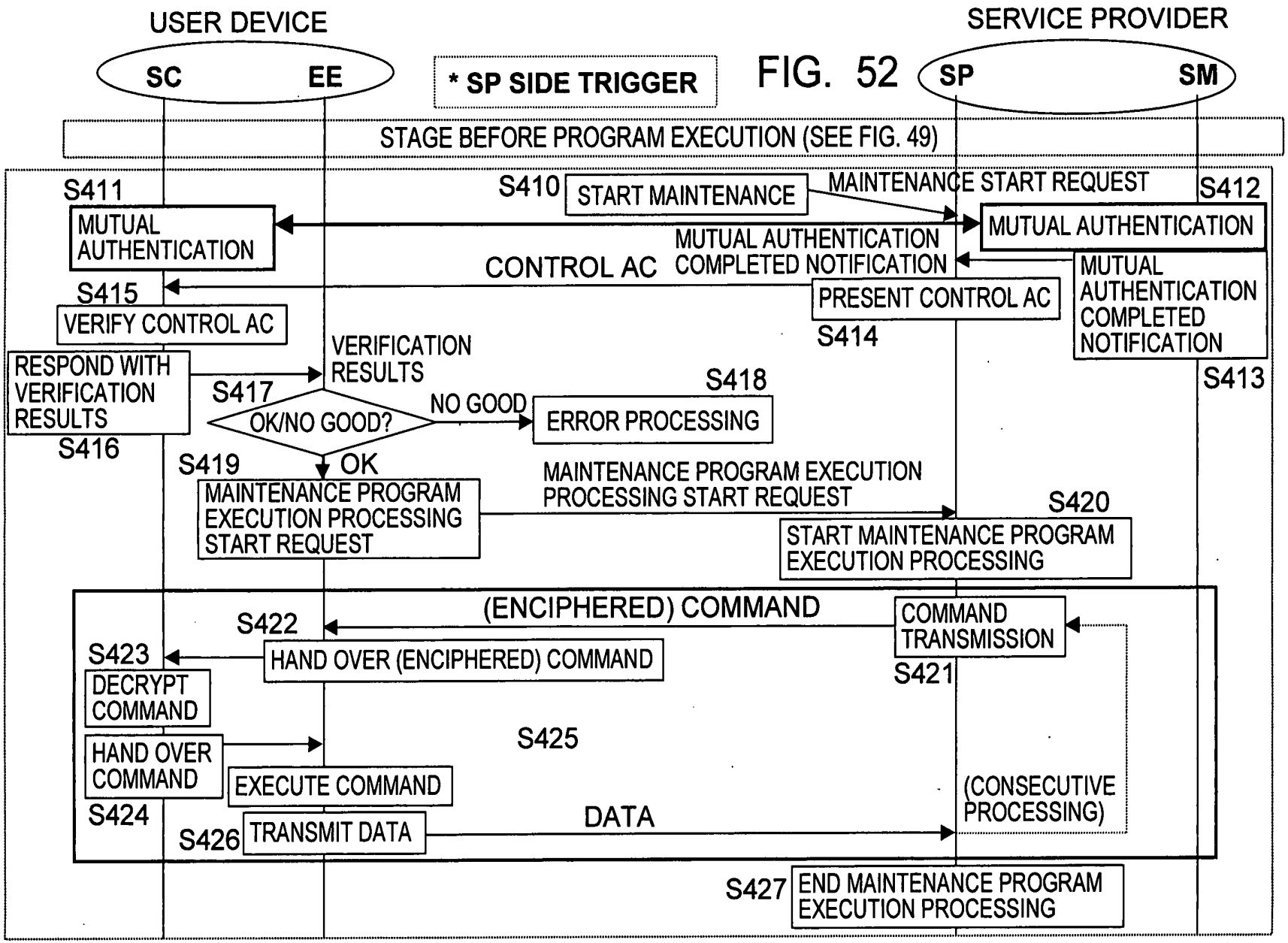


FIG. 52

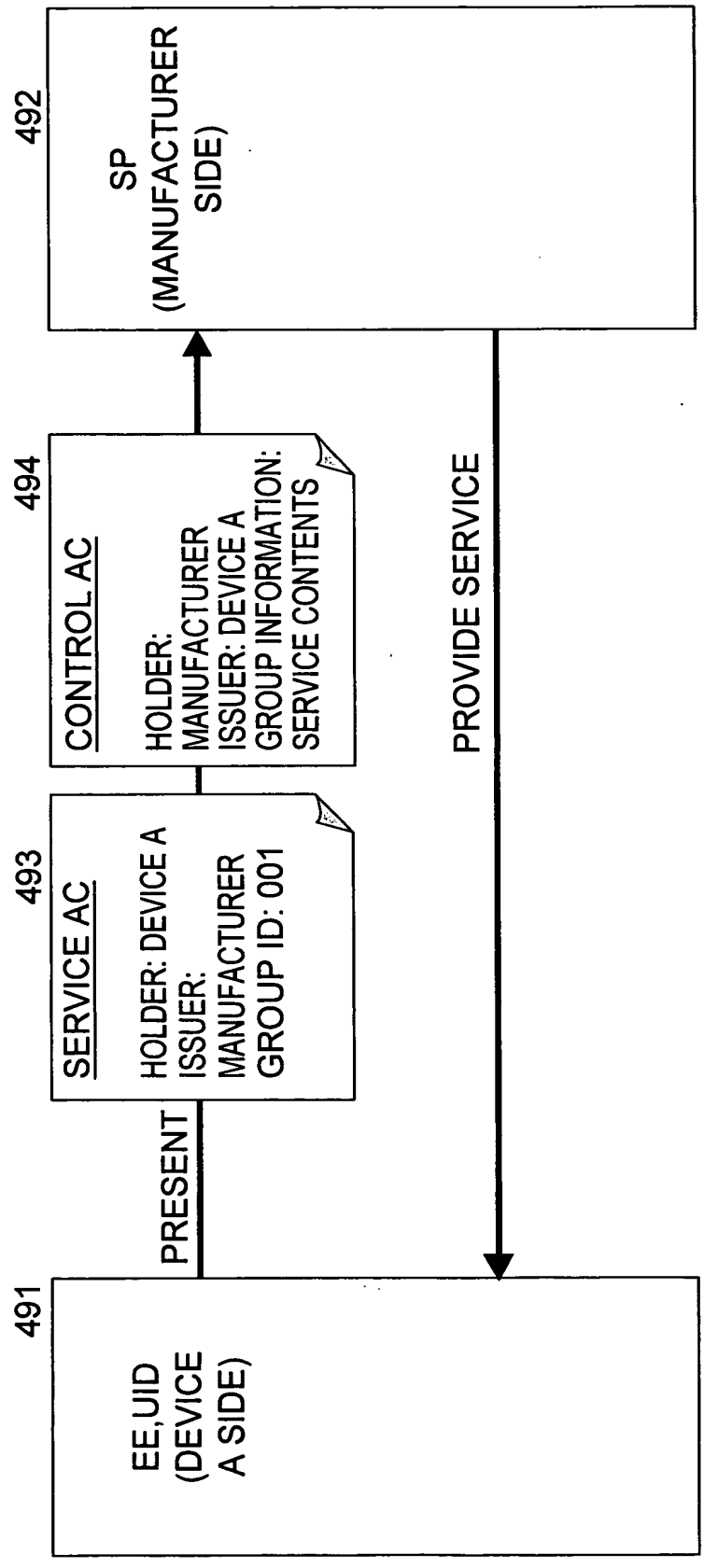

492
SP
(MANUFACTURER
SIDE)
494
CONTROL AC
HOLDER:
MANUFACTURER
ISSUER: DEVICE A
GROUP INFORMATION:
SERVICE CONTENTS
493
SERVICE AC
HOLDER: DEVICE A
ISSUER:
MANUFACTURER
GROUP ID: 001
PRESENT
PROVIDE SERVICE
491
EE,UID
(DEVICE
A SIDE)

FIG. 53

	ISSUER	ISSUING TIMING	HOLDER	VERIFIER	ATTRIBUTE
AC01	CHAT ADMINISTRATOR (SP)	AT LOGIN	MR. A UID_USC or EE_SC	SP_SM	SP SERVER ACCESS PRIVILEGES
AC02	MR. B (SP)	AT LOGIN	MR. A UID_USC or EE_SC	MR. B UID_USC or EE_SC	MR. B SERVER ACCESS PRIVILEGES

FIG. 54

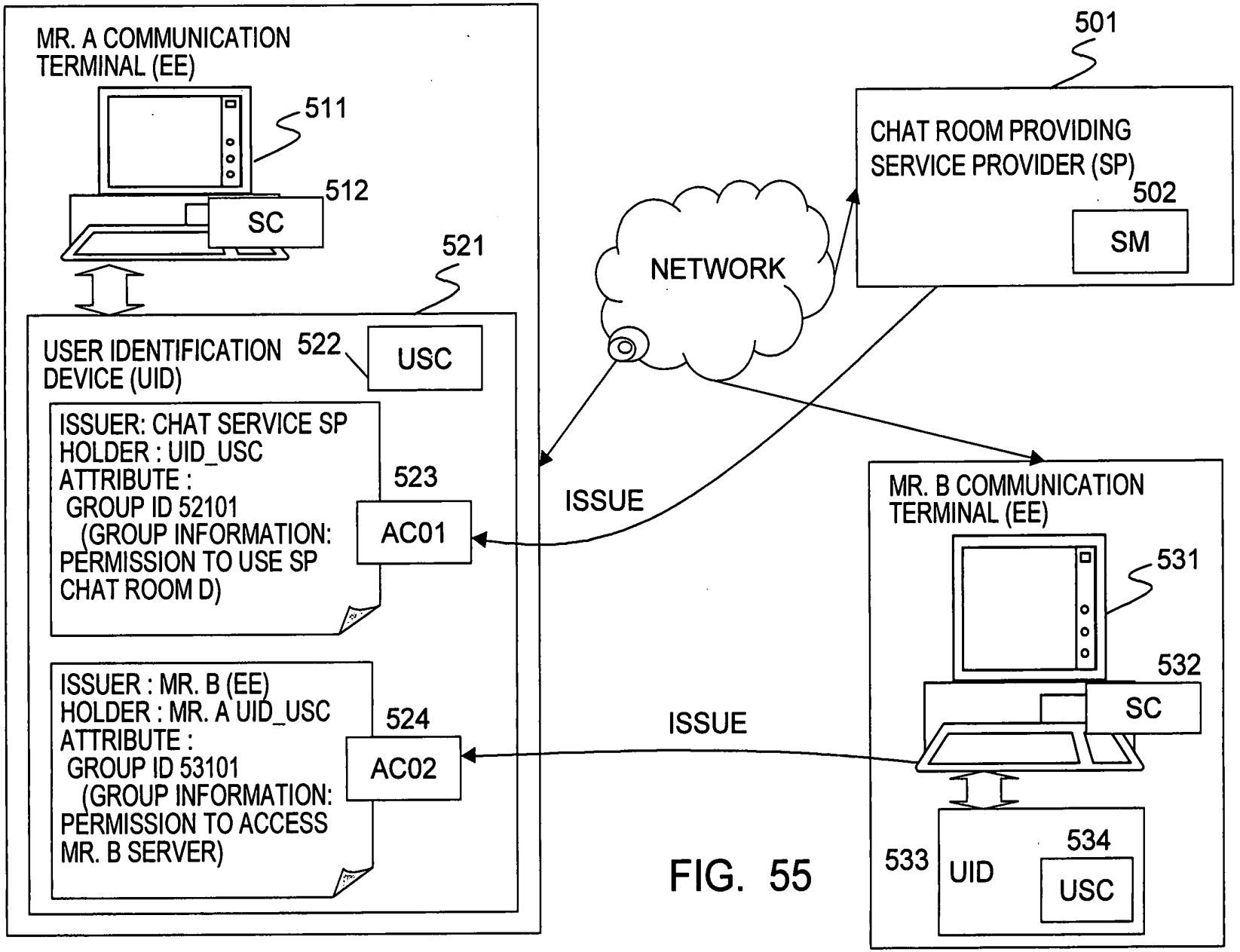


FIG. 55

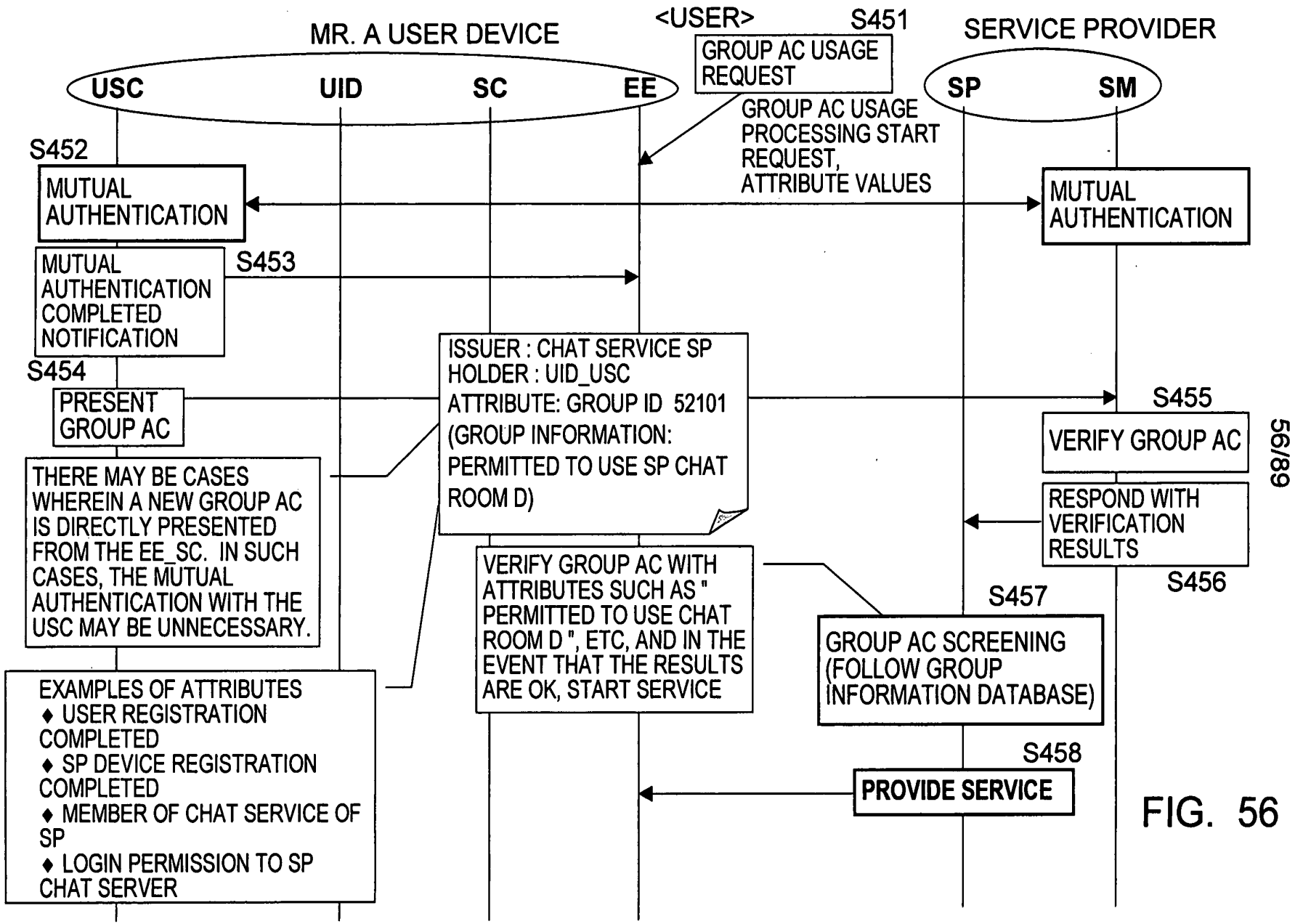


FIG. 56

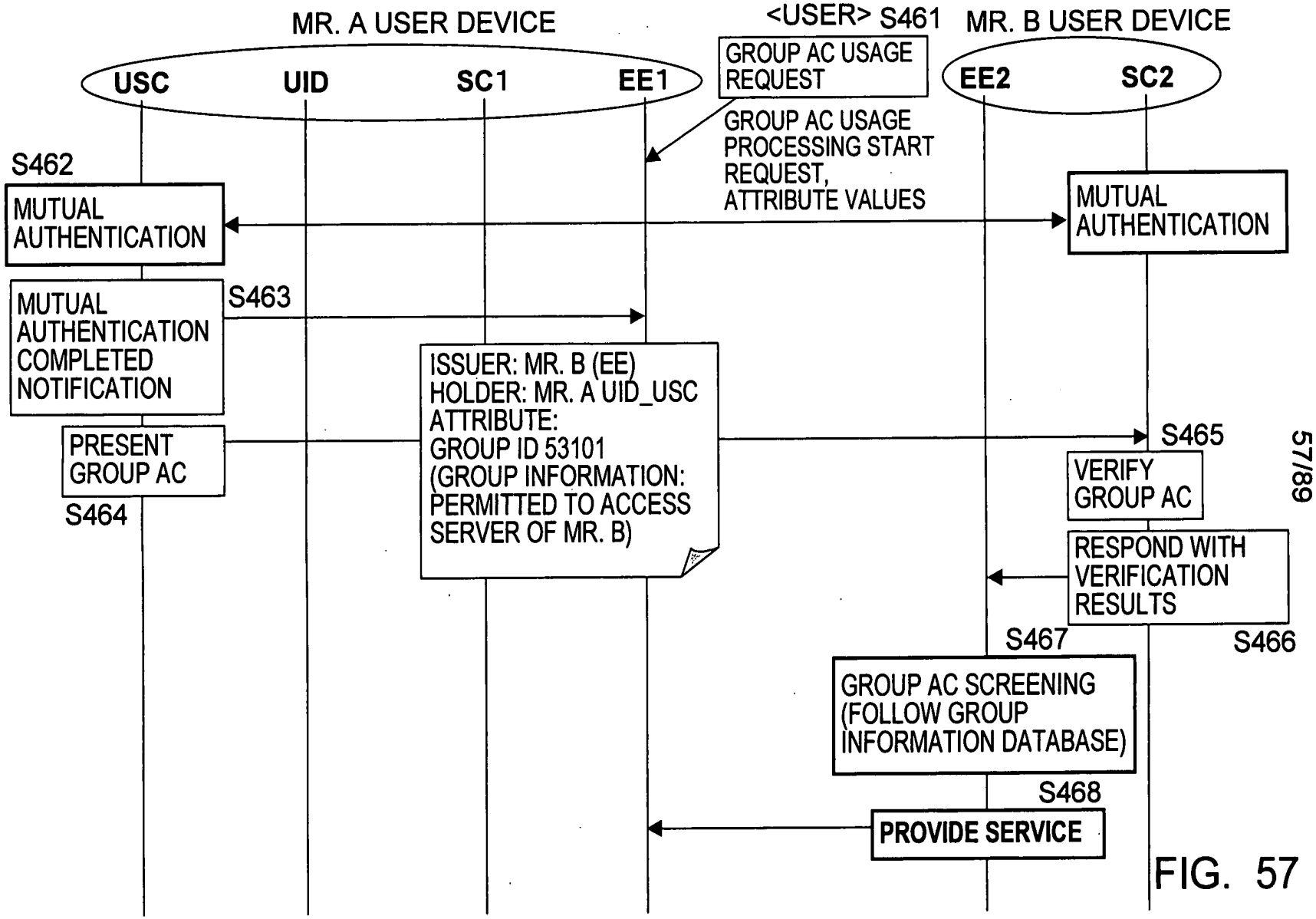


FIG. 57

57/89

10/517060

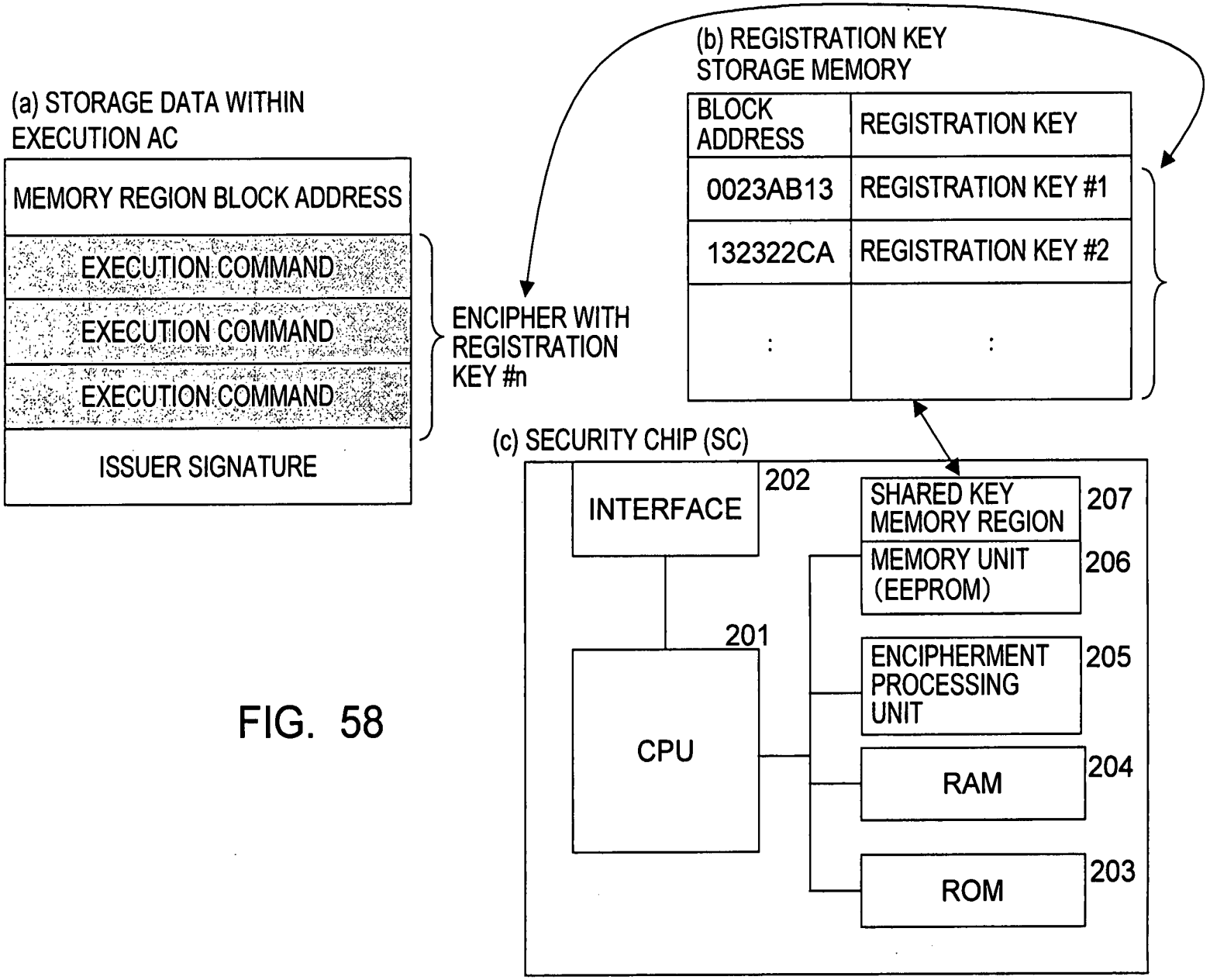
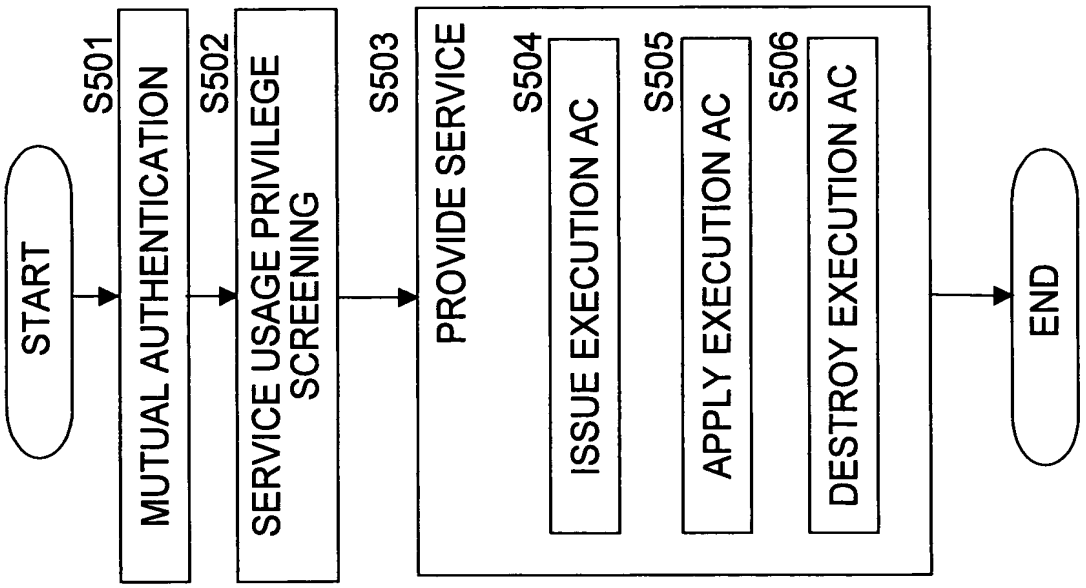


FIG. 58

FIG. 59


START
S501
MUTUAL AUTHENTICATION
S502
SERVICE USAGE PRIVILEGE SCREENING
S503
PROVIDE SERVICE
S504
ISSUE EXECUTION AC
S505
APPLY EXECUTION AC
S506
DESTROY EXECUTION AC
END

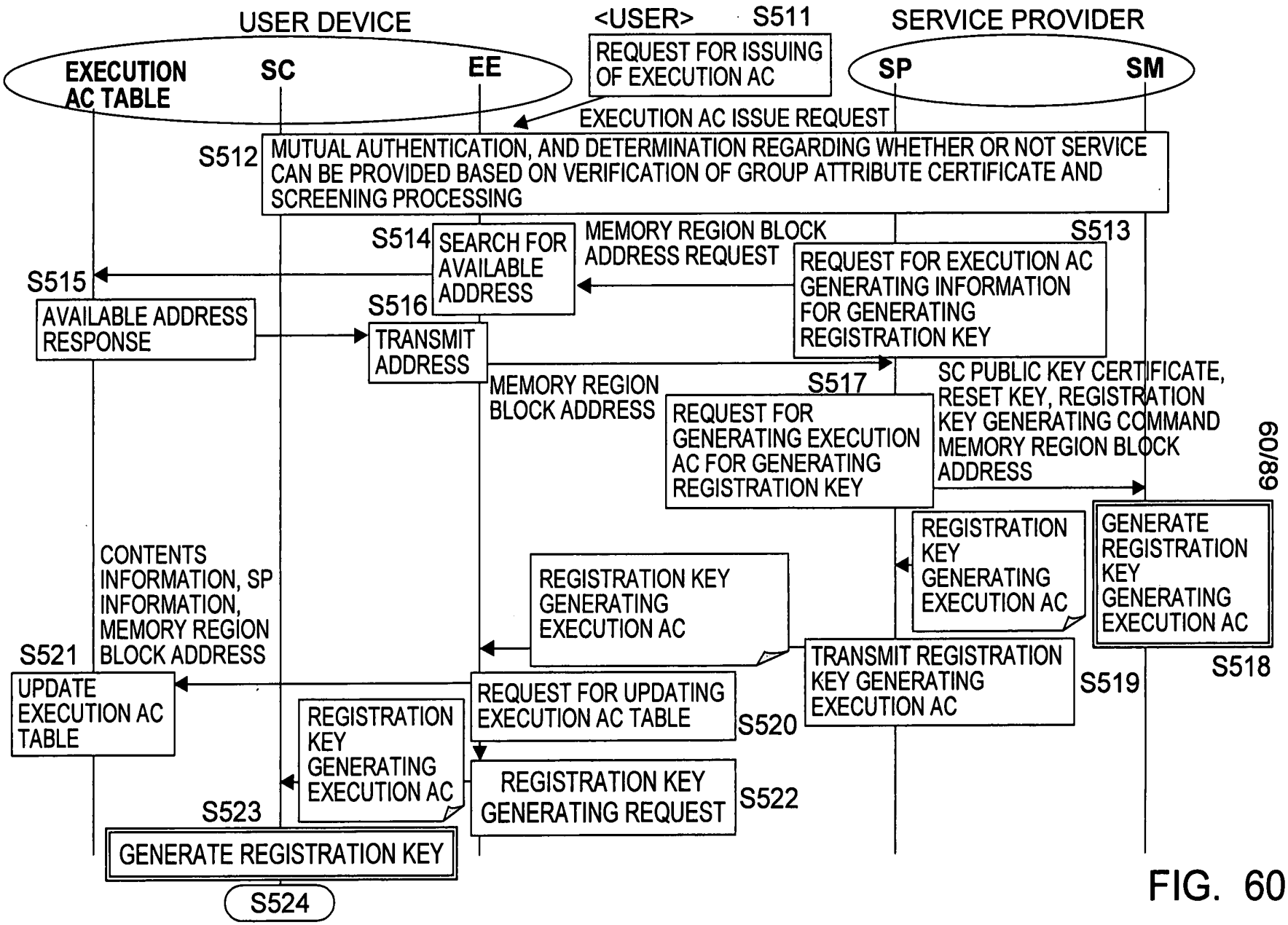


FIG. 60

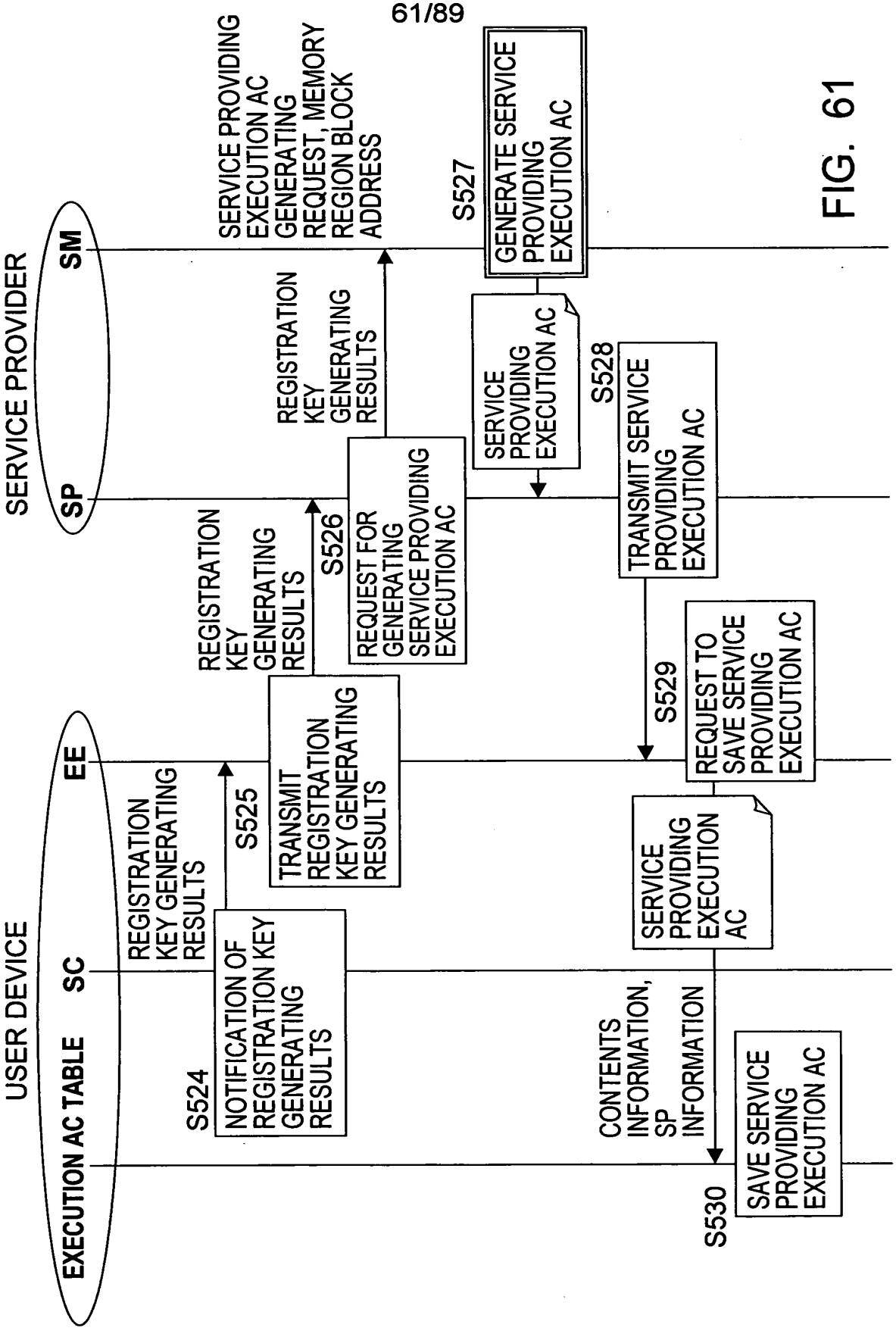

USER DEVICE
EXECUTION AC TABLE
SC
EE
SERVICE PROVIDER
SP
SM
REGISTRATION KEY GENERATING RESULTS
S524
NOTIFICATION OF REGISTRATION KEY GENERATING RESULTS
S525
TRANSMIT REGISTRATION KEY GENERATING RESULTS
REGISTRATION KEY GENERATING RESULTS
S526
REQUEST FOR GENERATING SERVICE PROVIDING EXECUTION AC
SERVICE PROVIDING EXECUTION AC
S527
GENERATE SERVICE PROVIDING EXECUTION AC
SERVICE PROVIDING EXECUTION AC
S528
TRANSMIT SERVICE PROVIDING EXECUTION AC
S529
REQUEST TO SAVE SERVICE PROVIDING EXECUTION AC
SERVICE PROVIDING EXECUTION AC
CONTENTS INFORMATION, SP INFORMATION
S530
SAVE SERVICE PROVIDING EXECUTION AC

FIG. 61

SP INFORMATION	ENCIPHERED DATA (e.g., CONTENTS) INFORMATION	ENCIPHERED DATA (CONTENTS) DECIPHERING PROCESSING APPLICATION EXECUTION AC
SP_1	ENCIPHERED DATA 1	EXECUTION AC 0001
	ENCIPHERED DATA 2	EXECUTION AC 0002
SP_2	ENCIPHERED DATA 11	. . .
	ENCIPHERED DATA 12	
	ENCIPHERED DATA 13	

FIG. 62

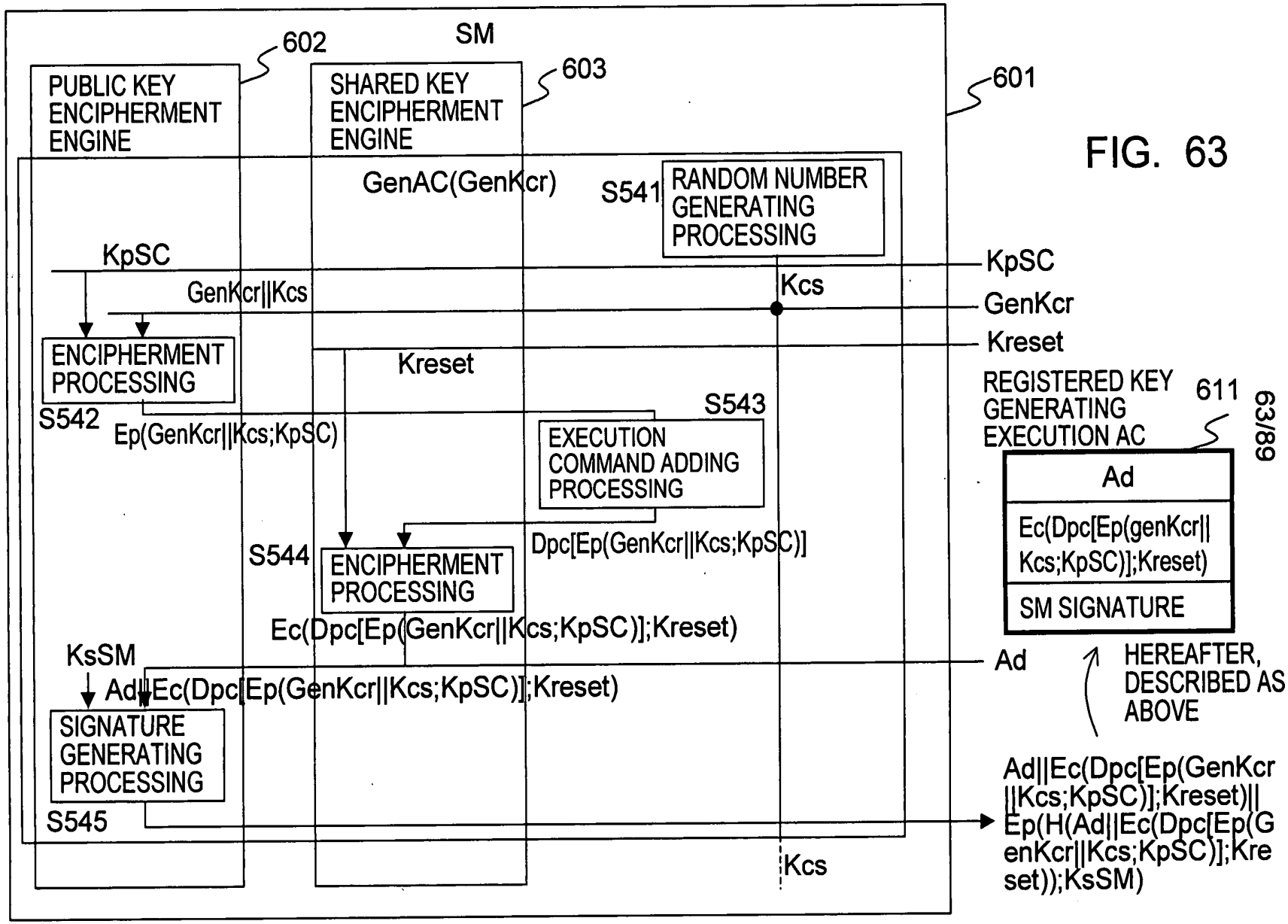


FIG. 63

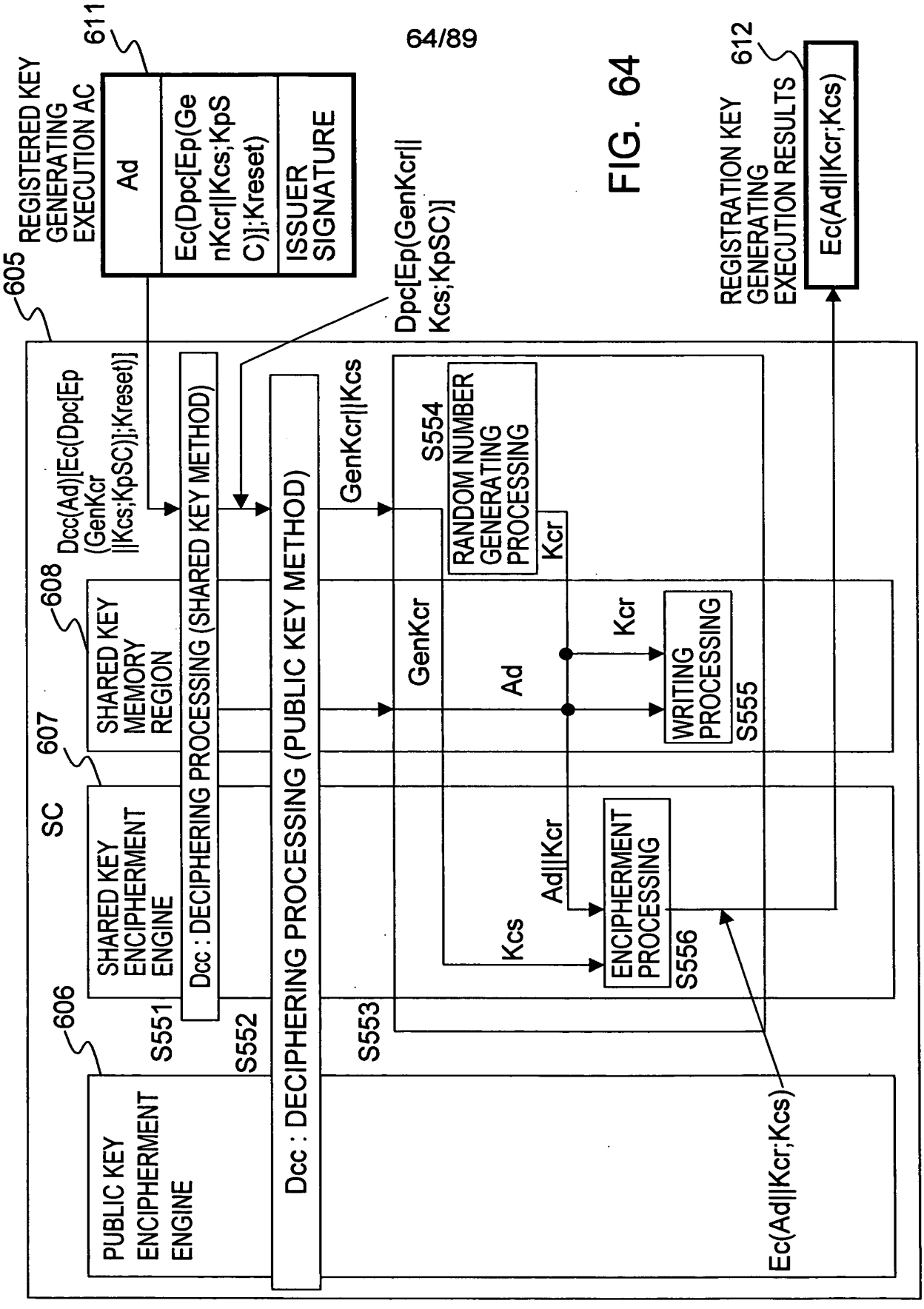
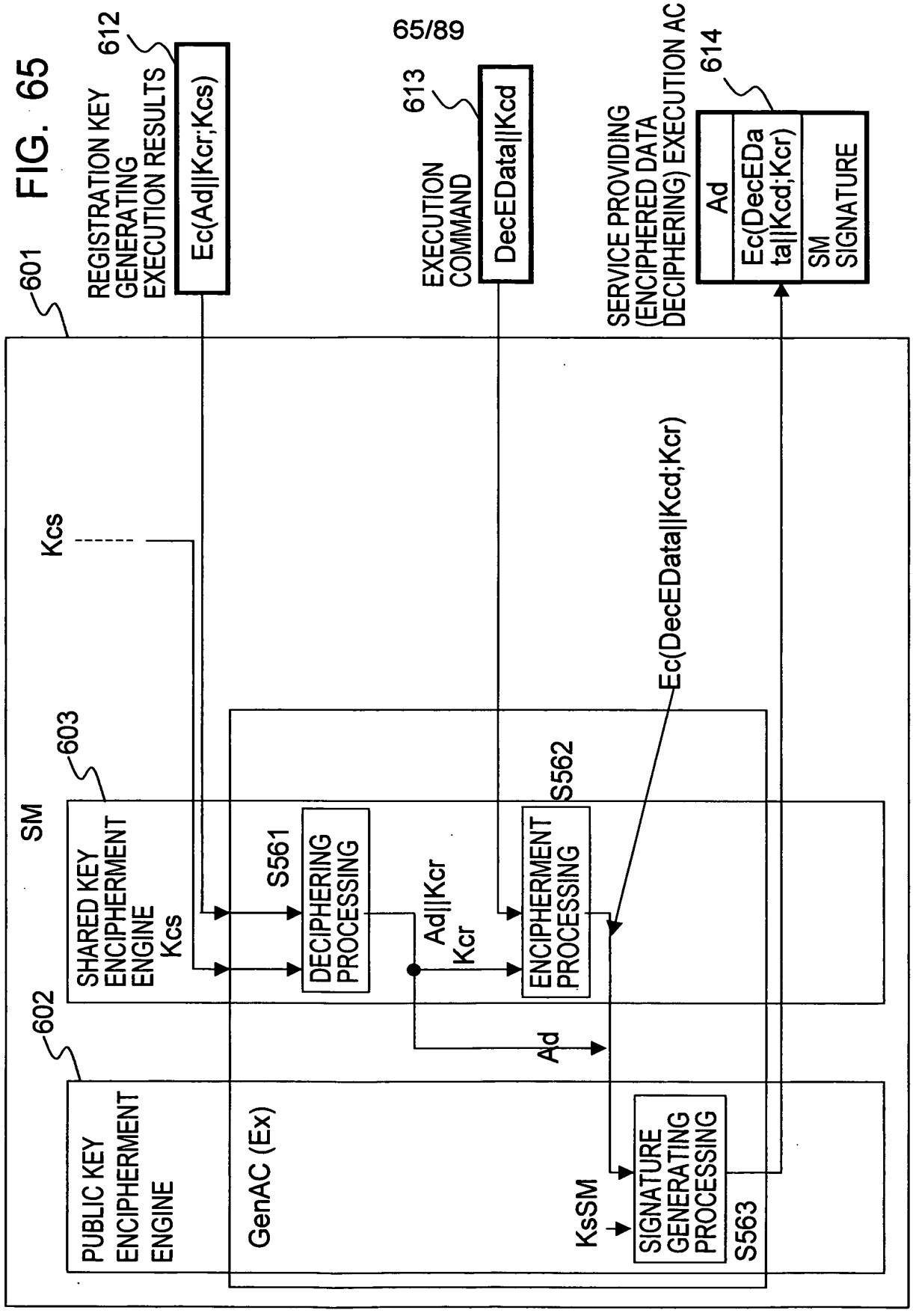

611
REGISTERED KEY GENERATING EXECUTION AC
Ad
Ec(Dpc[Ep(GenKcr||Kcs;KpSC)];Kreset)
ISSUER SIGNATURE
605
Dpc[Ep(GenKcr||Kcs;KpSC)]
612
REGISTRATION KEY GENERATING EXECUTION RESULTS
Ec(Ad||Kcr;Kcs)
SC
607
608
SHARED KEY ENCIPHERMENT ENGINE
SHARED KEY MEMORY REGION
Dcc(Ad)[Ec(Dpc[Ep(GenKcr||Kcs;KpSC)];Kreset)]
Dcc : DECIPHERING PROCESSING (SHARED KEY METHOD)
GenKcr||Kcs
S554
RANDOM NUMBER GENERATING PROCESSING
Kcr
GenKcr
Ad
Kcr
WRITING PROCESSING
S555
Kcs
Ad||Kcr
ENCIPHERMENT PROCESSING
S556
606
PUBLIC KEY ENCIPHERMENT ENGINE
S551
S552
S553
Dcc : DECIPHERING PROCESSING (PUBLIC KEY METHOD)
Ec(Ad||Kcr;Kcs)

FIG. 64

FIG. 65


601
SM
602
PUBLIC KEY ENCIPHERMENT ENGINE
603
SHARED KEY ENCIPHERMENT ENGINE
Kcs
Kcs
GenAC (Ex)
KsSM
Ad
Ad||Kcr
Kcr
S561
DECIPHERING PROCESSING
S562
ENCIPHERMENT PROCESSING
S563
SIGNATURE GENERATING PROCESSING
REGISTRATION KEY GENERATING EXECUTION RESULTS
612
Ec(Ad||Kcr;Kcs)
EXECUTION COMMAND
613
DecEData||Kcd
SERVICE PROVIDING (ENCIPHERED DATA DECIPHERING) EXECUTION AC
614
Ad
Ec(DecEData||Kcd;Kcr)
SM SIGNATURE
Ec(DecEData||Kcd;Kcr)

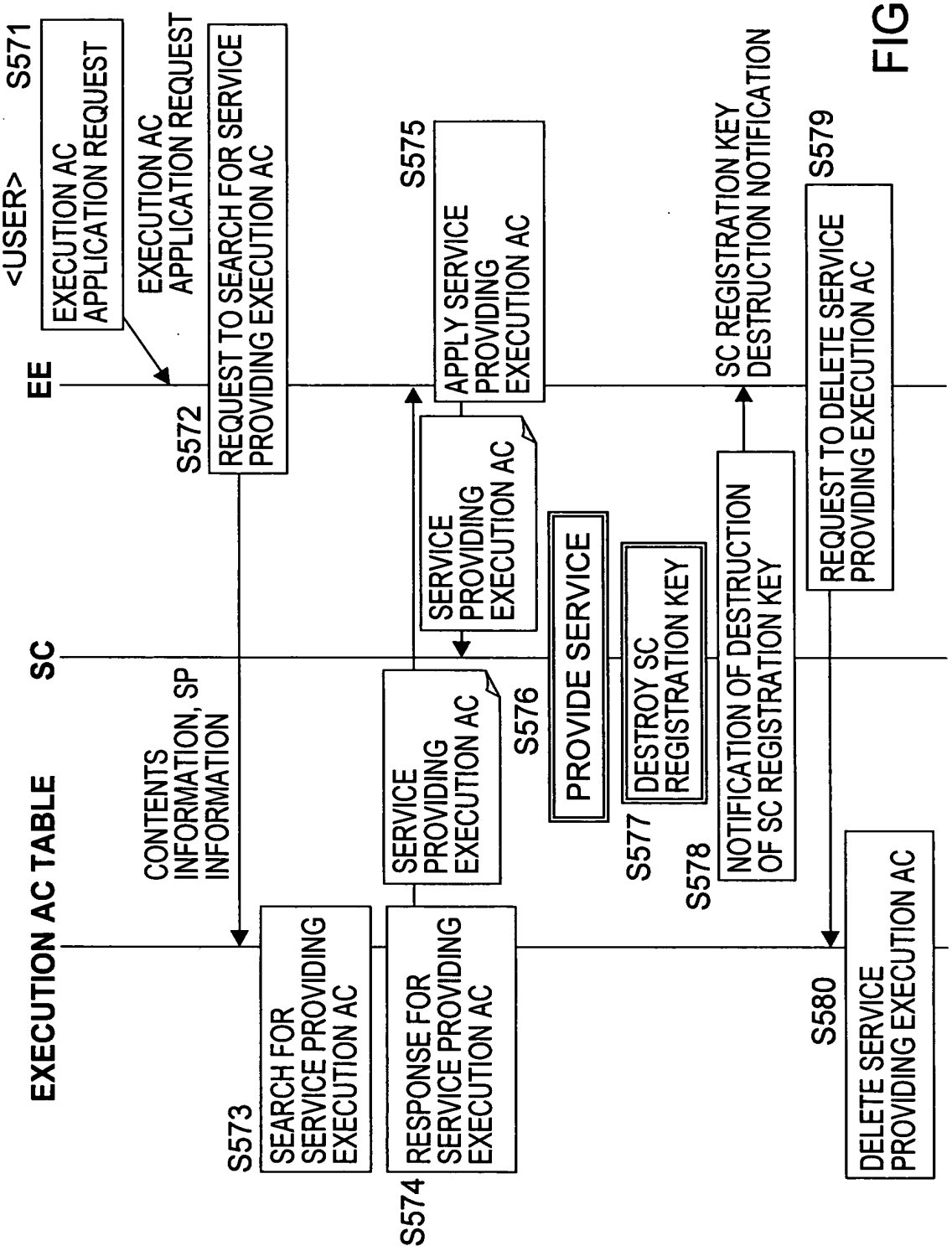

<USER>
EE
SC
EXECUTION AC TABLE
S571
EXECUTION AC APPLICATION REQUEST
EXECUTION AC APPLICATION REQUEST
S572
REQUEST TO SEARCH FOR SERVICE PROVIDING EXECUTION AC
CONTENTS INFORMATION, SP INFORMATION
S573
SEARCH FOR SERVICE PROVIDING EXECUTION AC
S574
RESPONSE FOR SERVICE PROVIDING EXECUTION AC
SERVICE PROVIDING EXECUTION AC
S575
APPLY SERVICE PROVIDING EXECUTION AC
SERVICE PROVIDING EXECUTION AC
S576
PROVIDE SERVICE
S577
DESTROY SC REGISTRATION KEY
S578
NOTIFICATION OF DESTRUCTION OF SC REGISTRATION KEY
SC REGISTRATION KEY DESTRUCTION NOTIFICATION
S579
REQUEST TO DELETE SERVICE PROVIDING EXECUTION AC
S580
DELETE SERVICE PROVIDING EXECUTION AC

FIG. 66

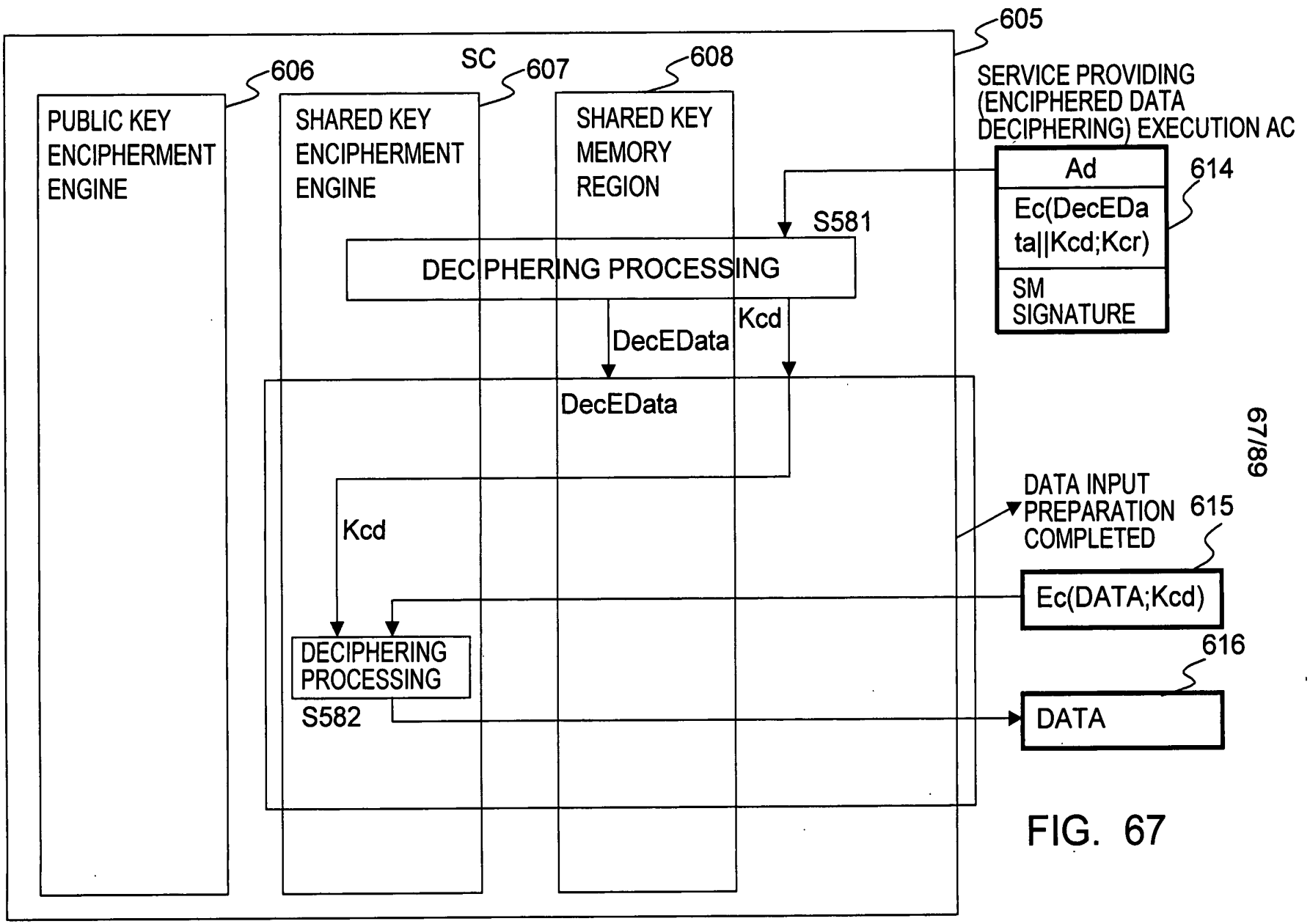


FIG. 67

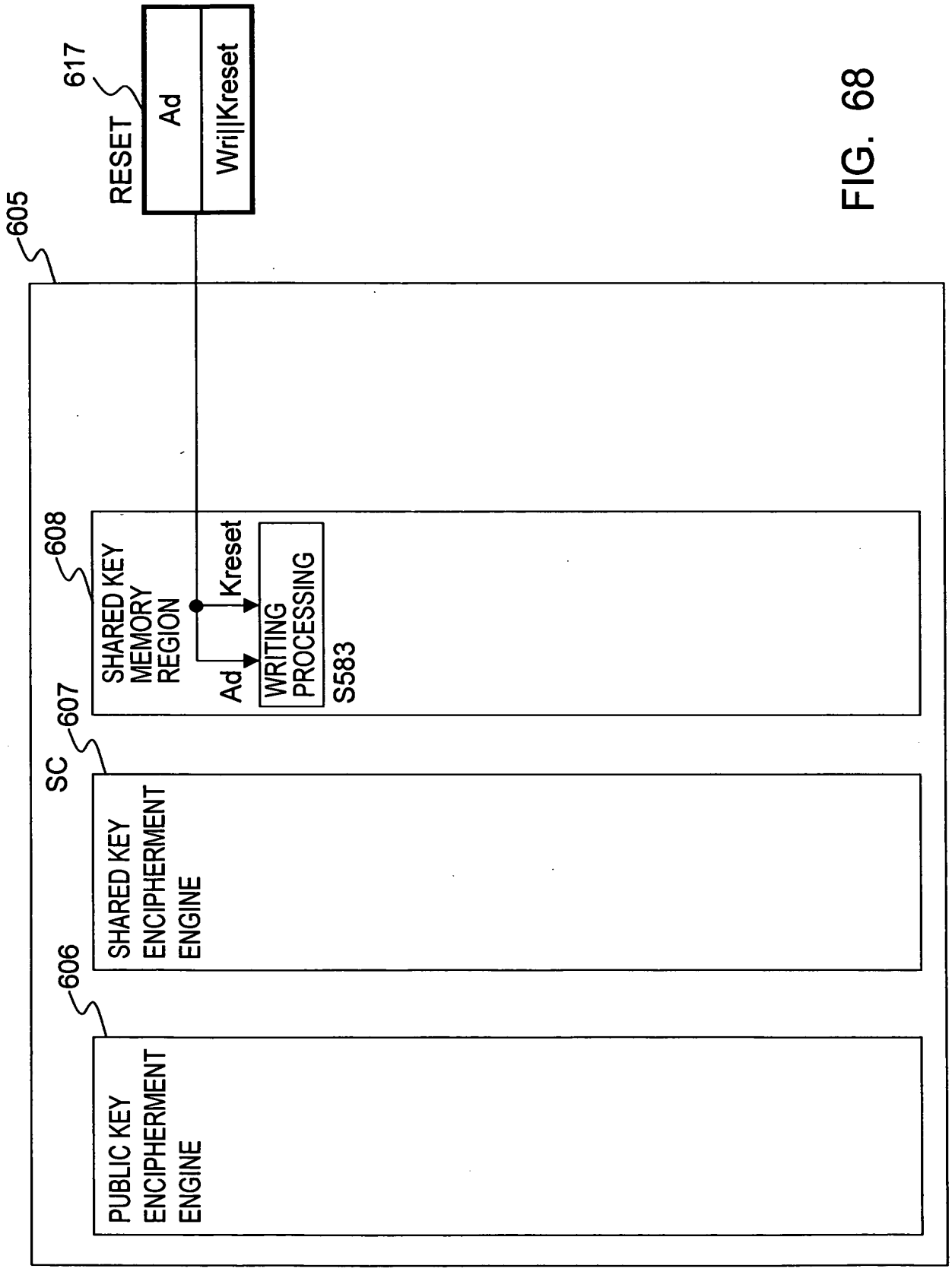

617
RESET
Ad
Wri||Kreset
605
608
SHARED KEY MEMORY REGION
Kreset
Ad
WRITING PROCESSING
S583
SC
607
SHARED KEY ENCIPHERMENT ENGINE
606
PUBLIC KEY ENCIPHERMENT ENGINE

FIG. 68

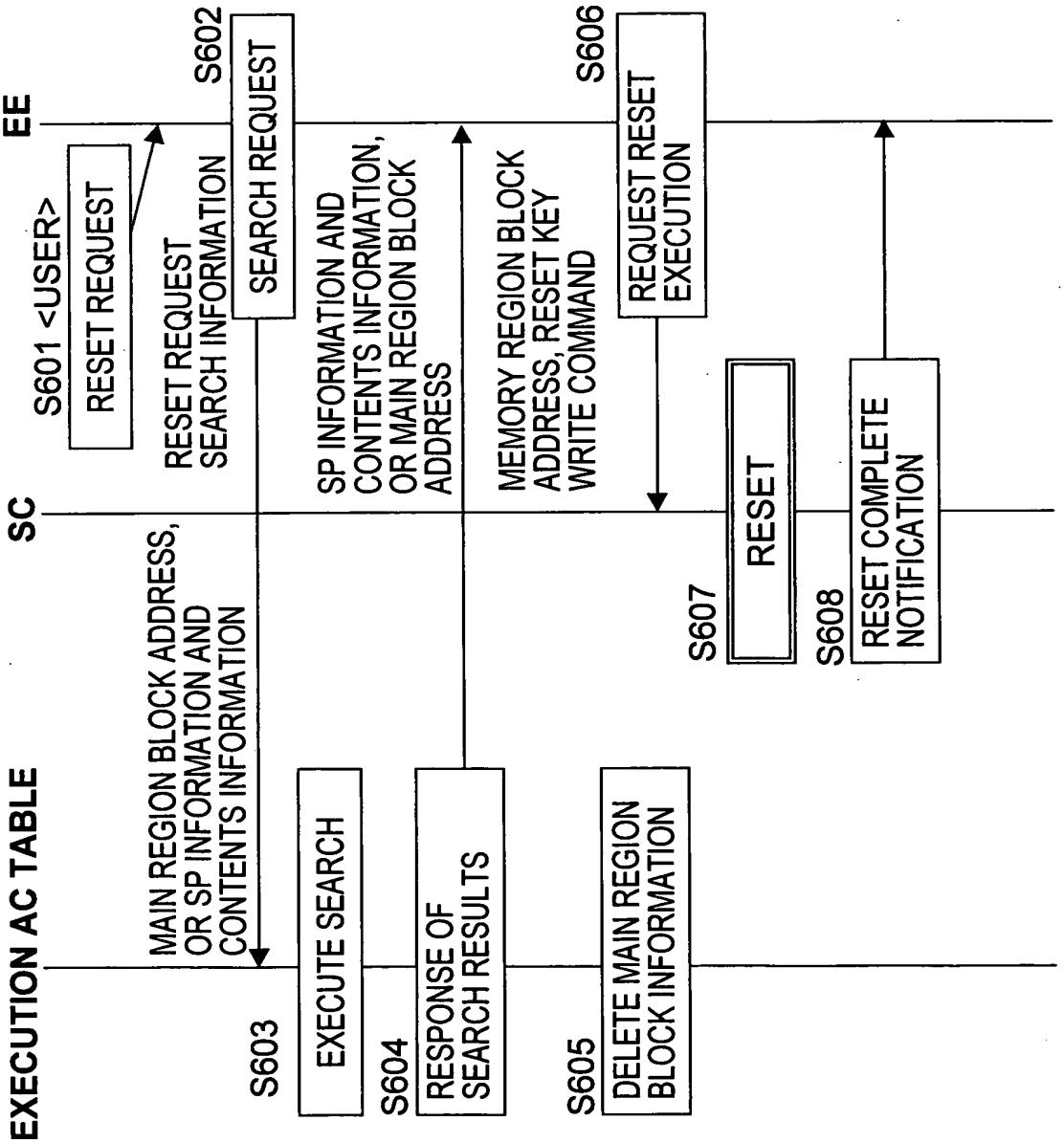

EE
SC
EXECUTION AC TABLE
S601 <USER>
RESET REQUEST
RESET REQUEST
SEARCH INFORMATION
S602
SEARCH REQUEST
SP INFORMATION AND
CONTENTS INFORMATION,
OR MAIN REGION BLOCK
ADDRESS
MEMORY REGION BLOCK
ADDRESS, RESET KEY
WRITE COMMAND
S606
REQUEST RESET
EXECUTION
MAIN REGION BLOCK ADDRESS,
OR SP INFORMATION AND
CONTENTS INFORMATION
S603
EXECUTE SEARCH
S604
RESPONSE OF
SEARCH RESULTS
S605
DELETE MAIN REGION
BLOCK INFORMATION
S607
RESET
S608
RESET COMPLETE
NOTIFICATION

FIG. 69

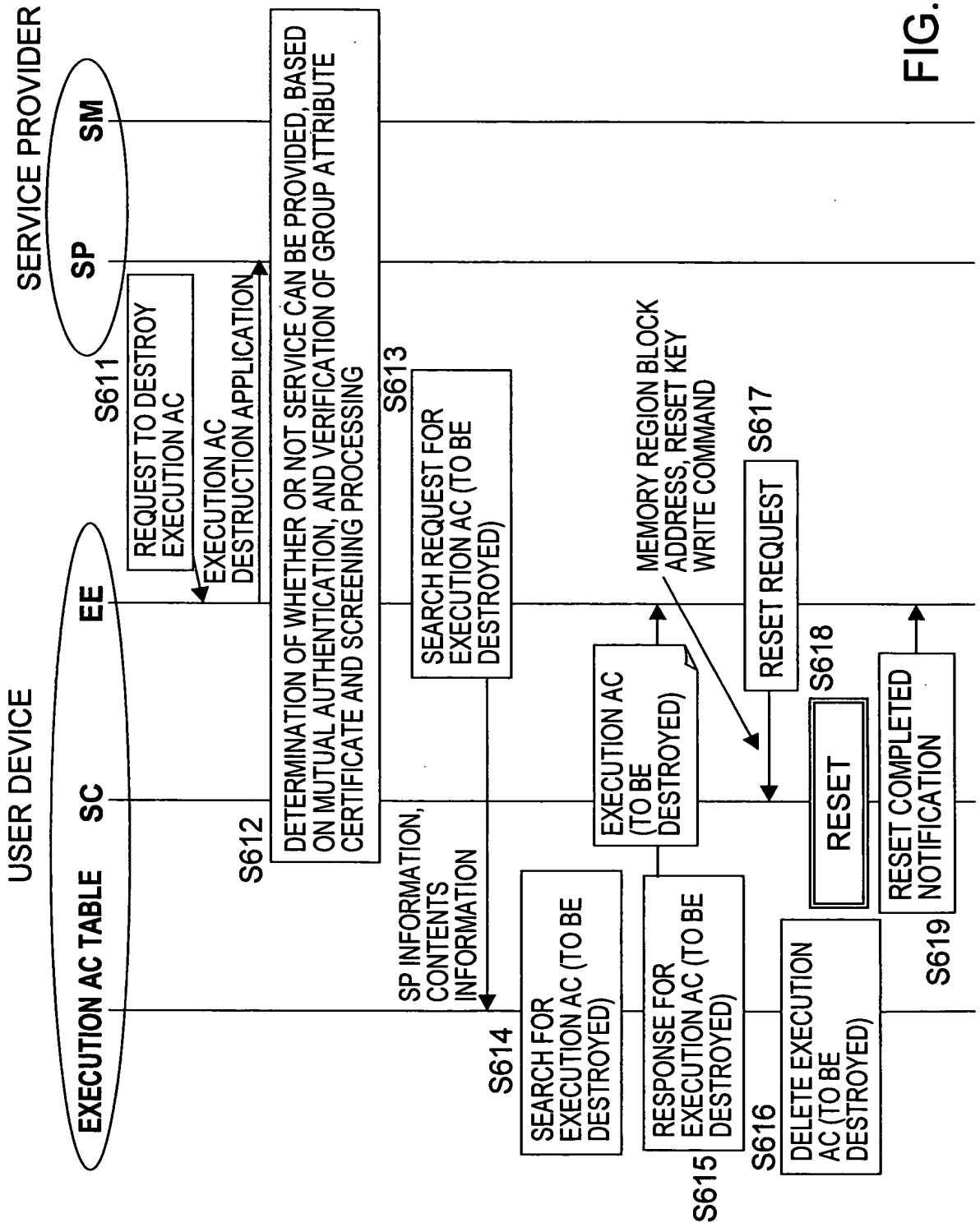
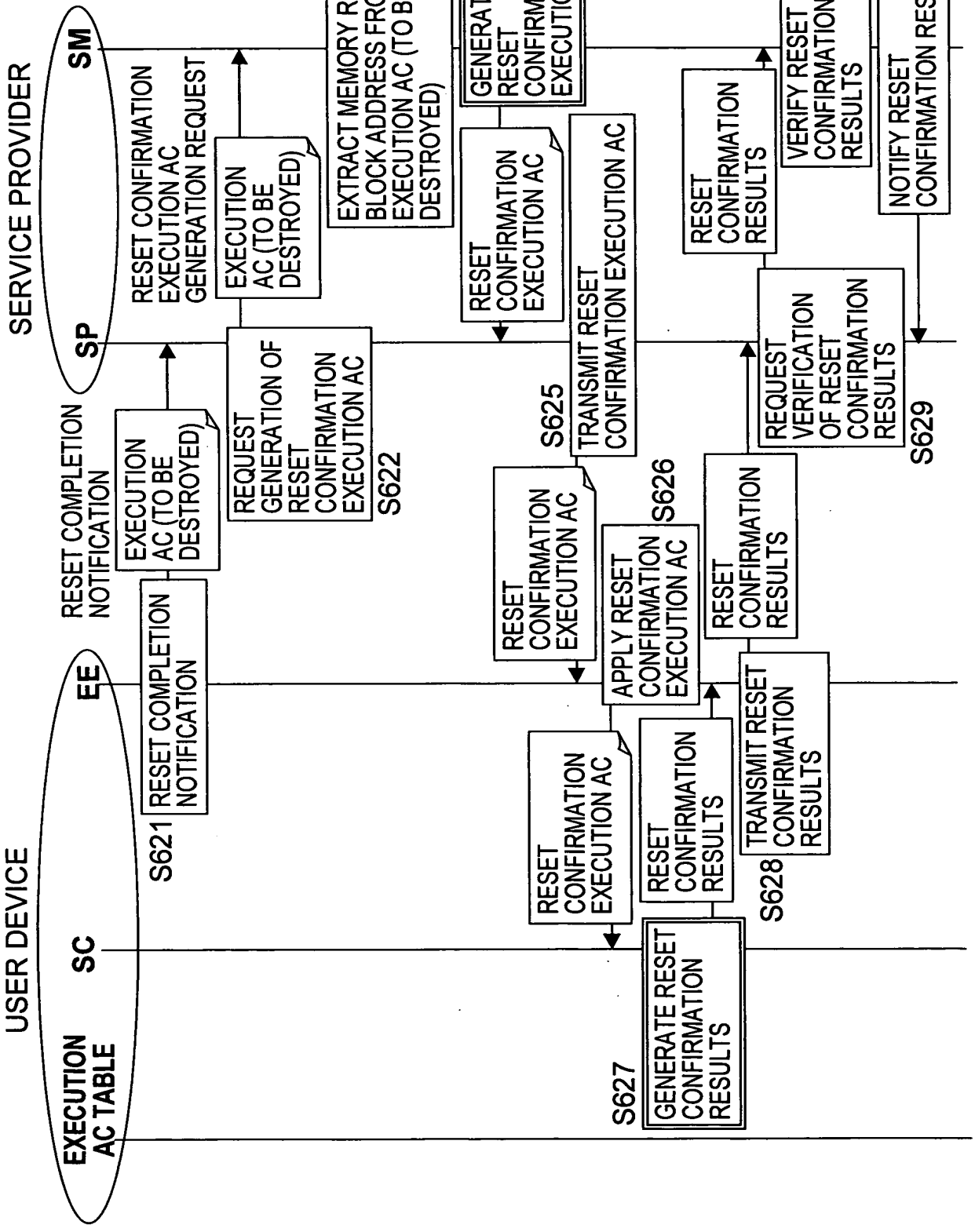

USER DEVICE
SERVICE PROVIDER
EXECUTION AC TABLE
SC
EE
SP
SM
S611
REQUEST TO DESTROY EXECUTION AC
EXECUTION AC DESTRUCTION APPLICATION
S612
DETERMINATION OF WHETHER OR NOT SERVICE CAN BE PROVIDED, BASED ON MUTUAL AUTHENTICATION, AND VERIFICATION OF GROUP ATTRIBUTE CERTIFICATE AND SCREENING PROCESSING
S613
SEARCH REQUEST FOR EXECUTION AC (TO BE DESTROYED)
SP INFORMATION, CONTENTS INFORMATION
S614
SEARCH FOR EXECUTION AC (TO BE DESTROYED)
S615
RESPONSE FOR EXECUTION AC (TO BE DESTROYED)
EXECUTION AC (TO BE DESTROYED)
MEMORY REGION BLOCK ADDRESS, RESET KEY WRITE COMMAND
S616
DELETE EXECUTION AC (TO BE DESTROYED)
S617
RESET REQUEST
S618
RESET
S619
RESET COMPLETED NOTIFICATION

FIG. 70

FIG. 71


USER DEVICE
SERVICE PROVIDER
EXECUTION AC TABLE
SC
EE
SP
SM
RESET COMPLETION NOTIFICATION
RESET COMPLETION NOTIFICATION
S621
EXECUTION AC (TO BE DESTROYED)
REQUEST GENERATION OF RESET CONFIRMATION EXECUTION AC
S622
RESET CONFIRMATION EXECUTION AC GENERATION REQUEST
EXECUTION AC (TO BE DESTROYED)
S623
EXTRACT MEMORY REGION BLOCK ADDRESS FROM EXECUTION AC (TO BE DESTROYED)
GENERATE RESET CONFIRMATION EXECUTION AC
S624
RESET CONFIRMATION EXECUTION AC
S625
TRANSMIT RESET CONFIRMATION EXECUTION AC
RESET CONFIRMATION EXECUTION AC
APPLY RESET CONFIRMATION EXECUTION AC
S626
RESET CONFIRMATION RESULTS
TRANSMIT RESET CONFIRMATION RESULTS
S628
RESET CONFIRMATION EXECUTION AC
RESET CONFIRMATION RESULTS
S627
GENERATE RESET CONFIRMATION RESULTS
RESET CONFIRMATION RESULTS
S630
VERIFY RESET CONFIRMATION RESULTS
NOTIFY RESET CONFIRMATION RESULTS
S631
REQUEST VERIFICATION OF RESET CONFIRMATION RESULTS
S629

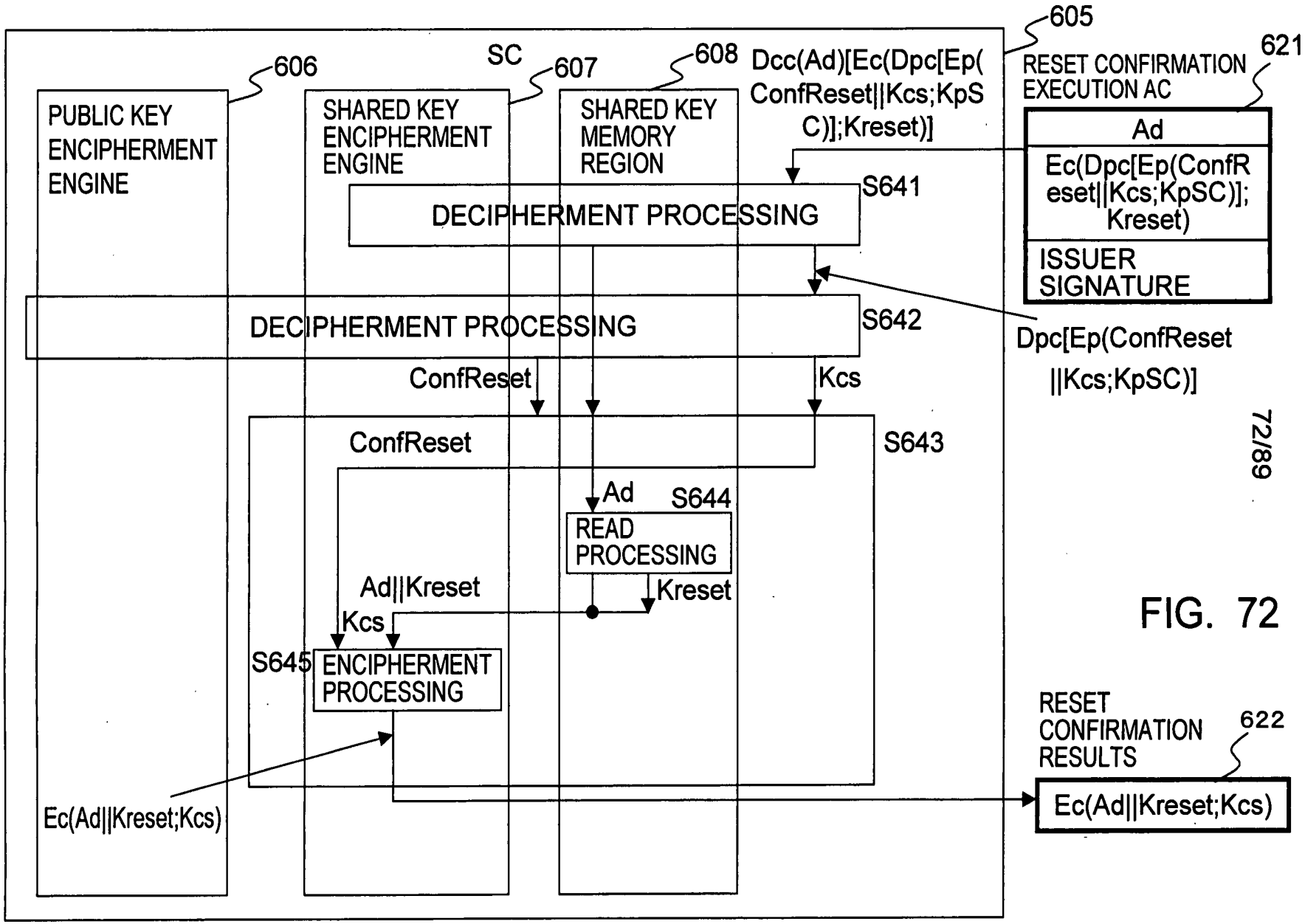


FIG. 72

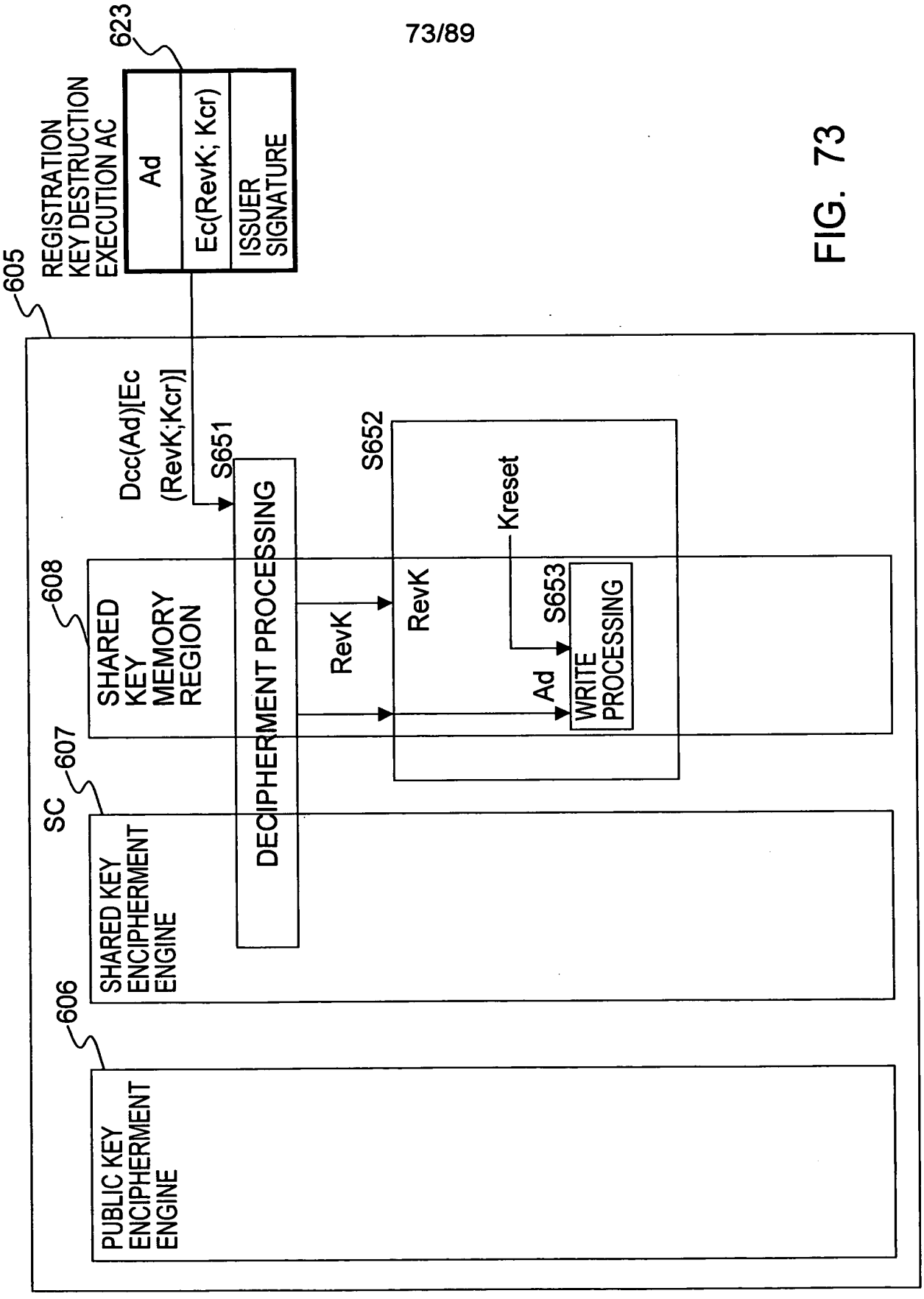

623
REGISTRATION KEY DESTRUCTION EXECUTION AC
Ad
Ec(RevK; Kcr)
ISSUER SIGNATURE
605
Dcc(Ad)[Ec (RevK;Kcr)]
S651
DECIPHERMENT PROCESSING
S652
Kreset
608
SHARED KEY MEMORY REGION
RevK
RevK
S653
Ad
WRITE PROCESSING
SC
607
SHARED KEY ENCIPHERMENT ENGINE
606
PUBLIC KEY ENCIPHERMENT ENGINE

FIG. 73

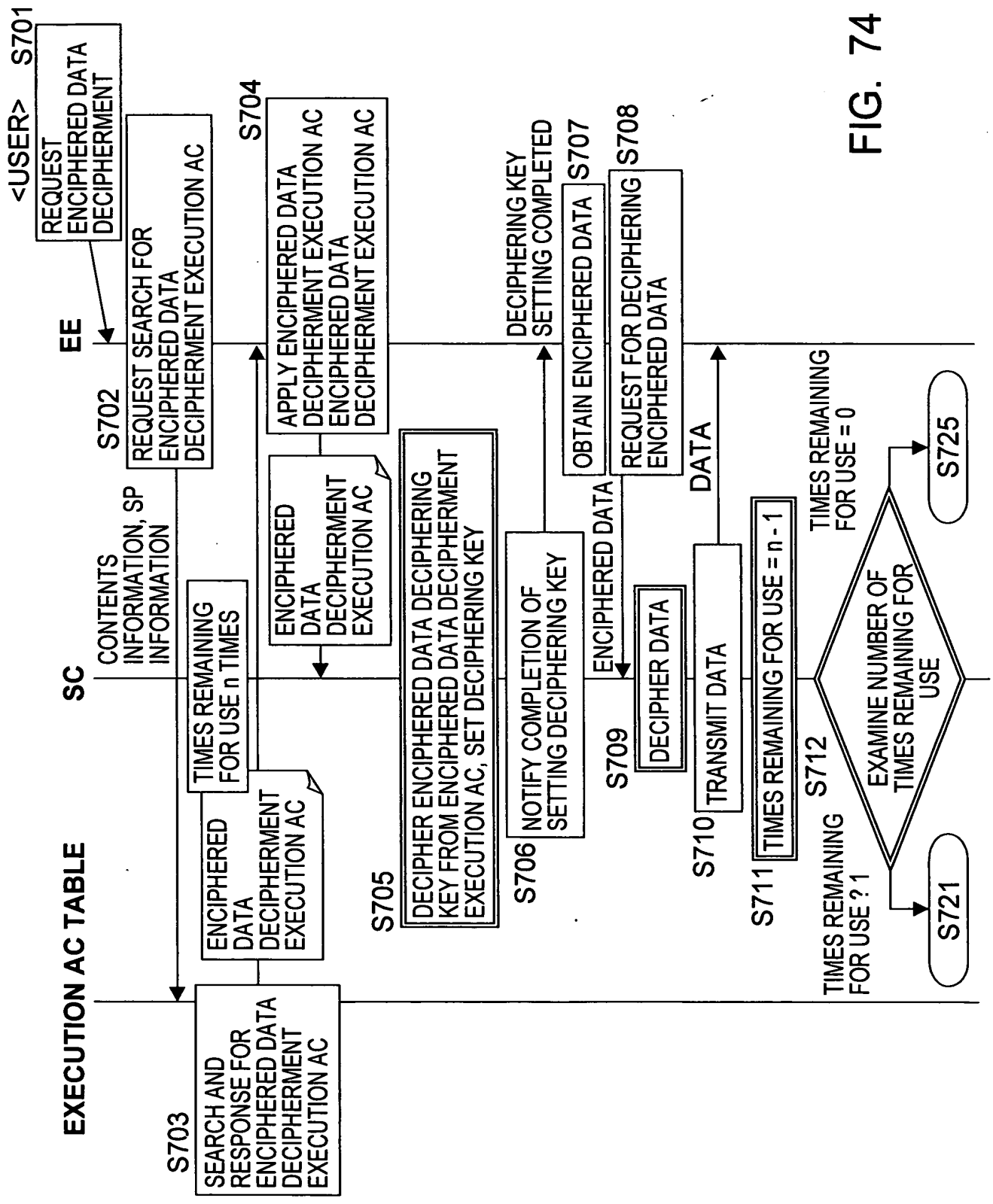

<USER>
S701
REQUEST ENCIPHERED DATA DECIPHERMENT
EE
S702
REQUEST SEARCH FOR ENCIPHERED DATA DECIPHERMENT EXECUTION AC
S704
APPLY ENCIPHERED DATA DECIPHERMENT EXECUTION AC
ENCIPHERED DATA DECIPHERMENT EXECUTION AC
DECIPHERING KEY SETTING COMPLETED
S707
OBTAIN ENCIPHERED DATA
S708
REQUEST FOR DECIPHERING ENCIPHERED DATA
SC
CONTENTS INFORMATION, SP INFORMATION
TIMES REMAINING FOR USE n TIMES
ENCIPHERED DATA DECIPHERMENT EXECUTION AC
S705
DECIPHER ENCIPHERED DATA DECIPHERING KEY FROM ENCIPHERED DATA DECIPHERMENT EXECUTION AC, SET DECIPHERING KEY
S706
NOTIFY COMPLETION OF SETTING DECIPHERING KEY
ENCIPHERED DATA
S709
DECIPHER DATA
DATA
S710
TRANSMIT DATA
S711
TIMES REMAINING FOR USE = n - 1
S712
EXAMINE NUMBER OF TIMES REMAINING FOR USE
TIMES REMAINING FOR USE = 0
S725
TIMES REMAINING FOR USE ? 1
S721
EXECUTION AC TABLE
S703
SEARCH AND RESPONSE FOR ENCIPHERED DATA DECIPHERMENT EXECUTION AC

FIG. 74

(A) CASE OF TIMES REMAINING FOR USE BEING 1 OR GREATER FOLLOWING DATA DECIPHERMENT (n ≥ 2)

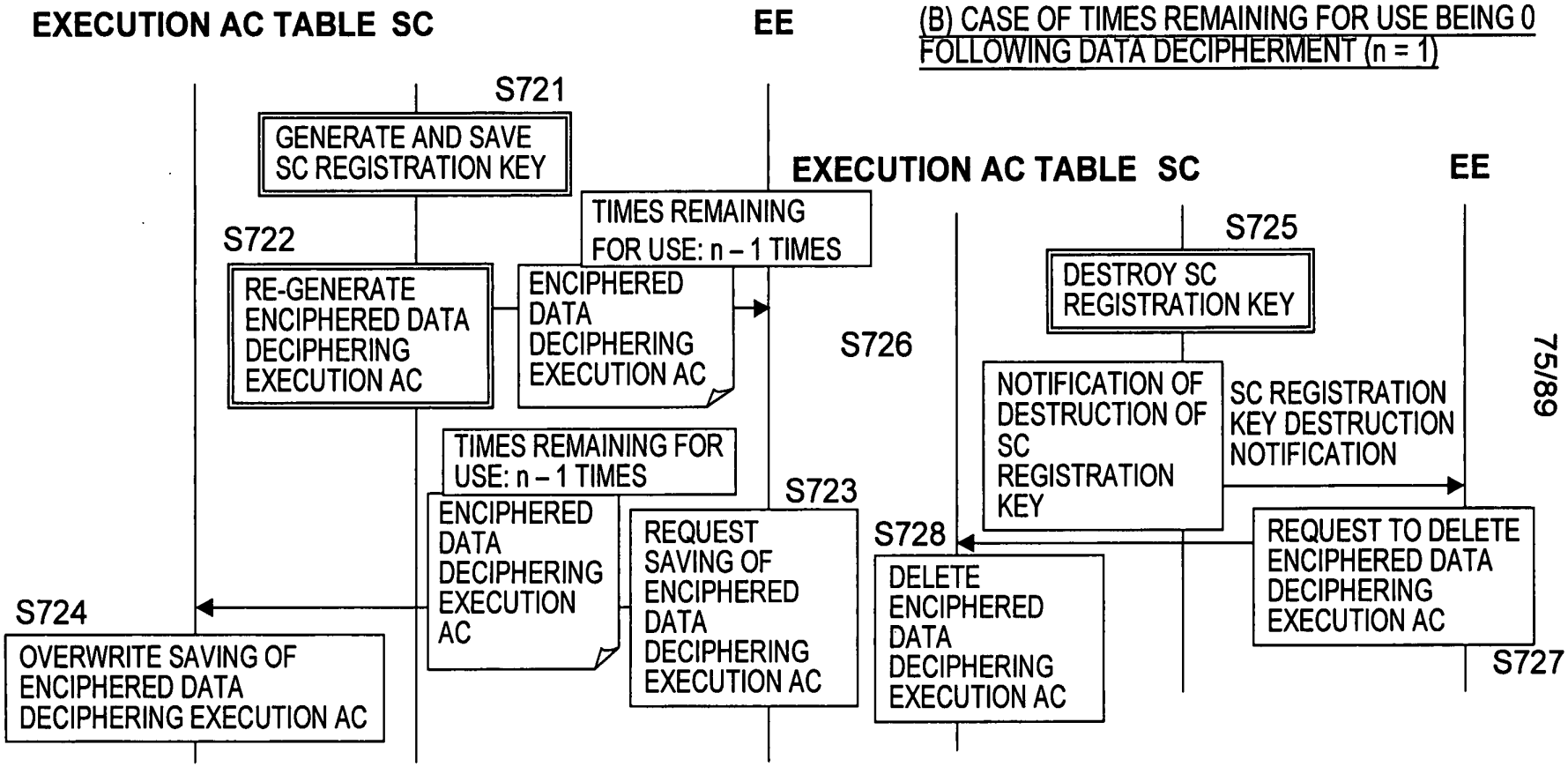


FIG. 75

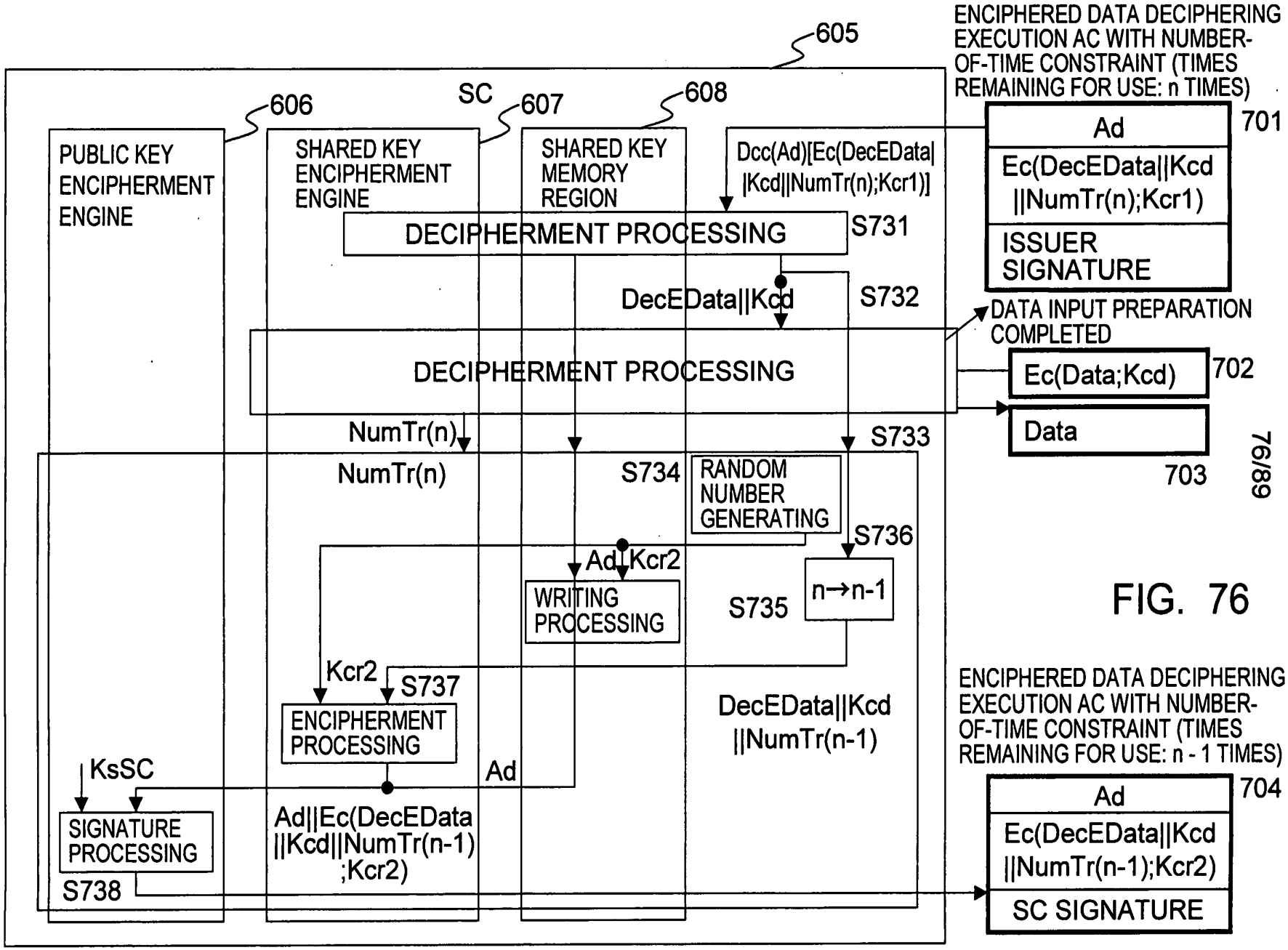


FIG. 76

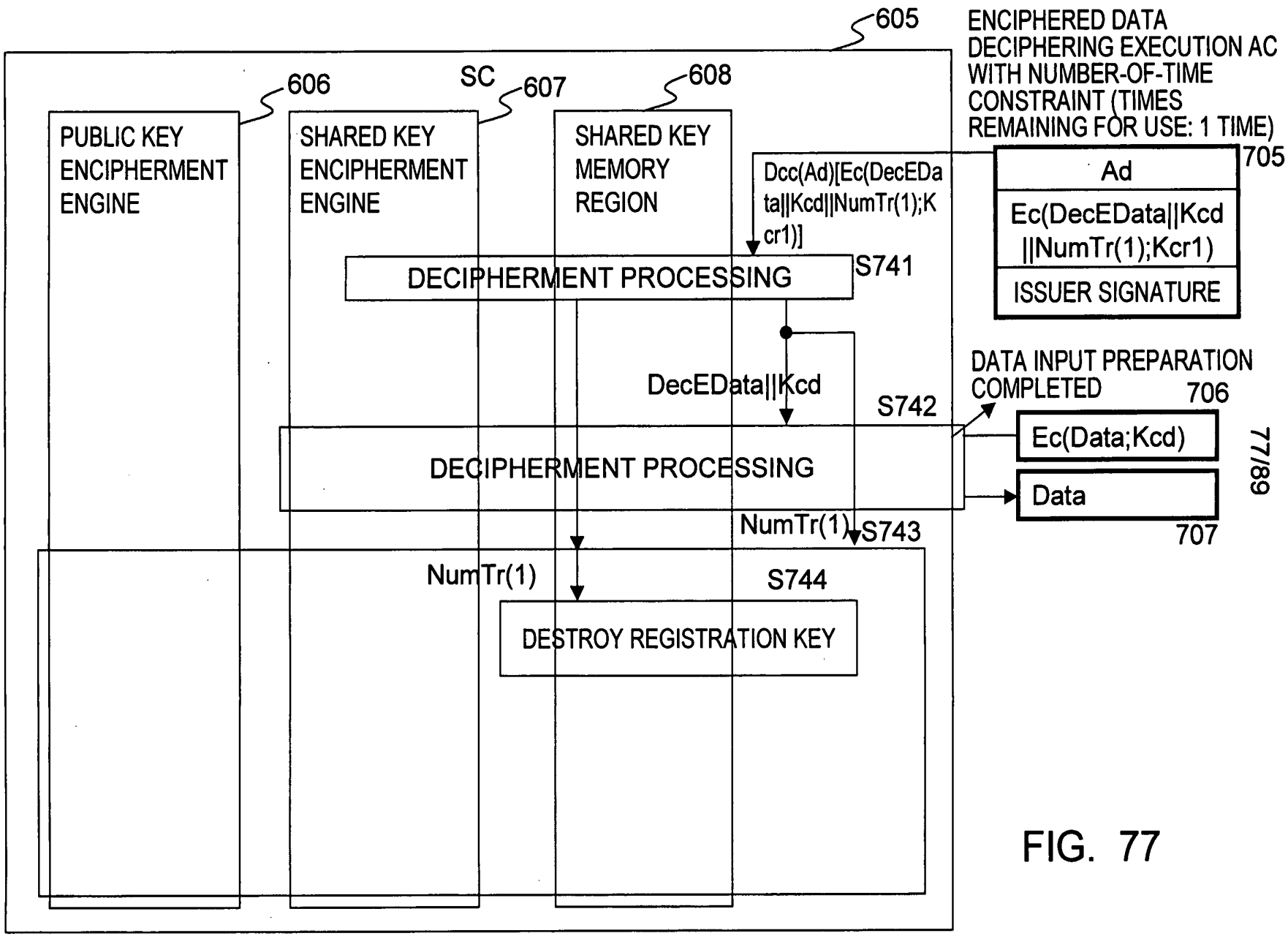


FIG. 77

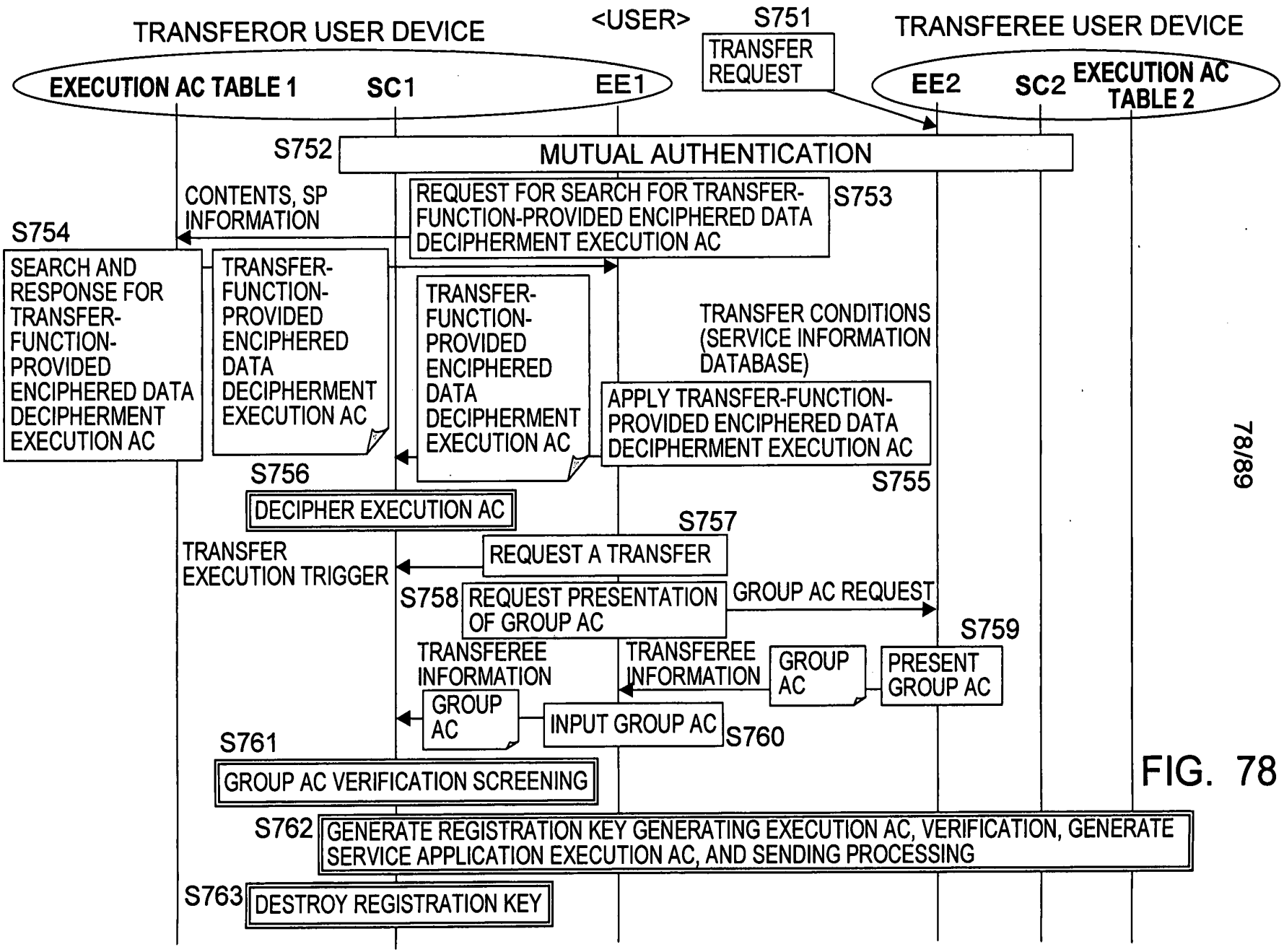
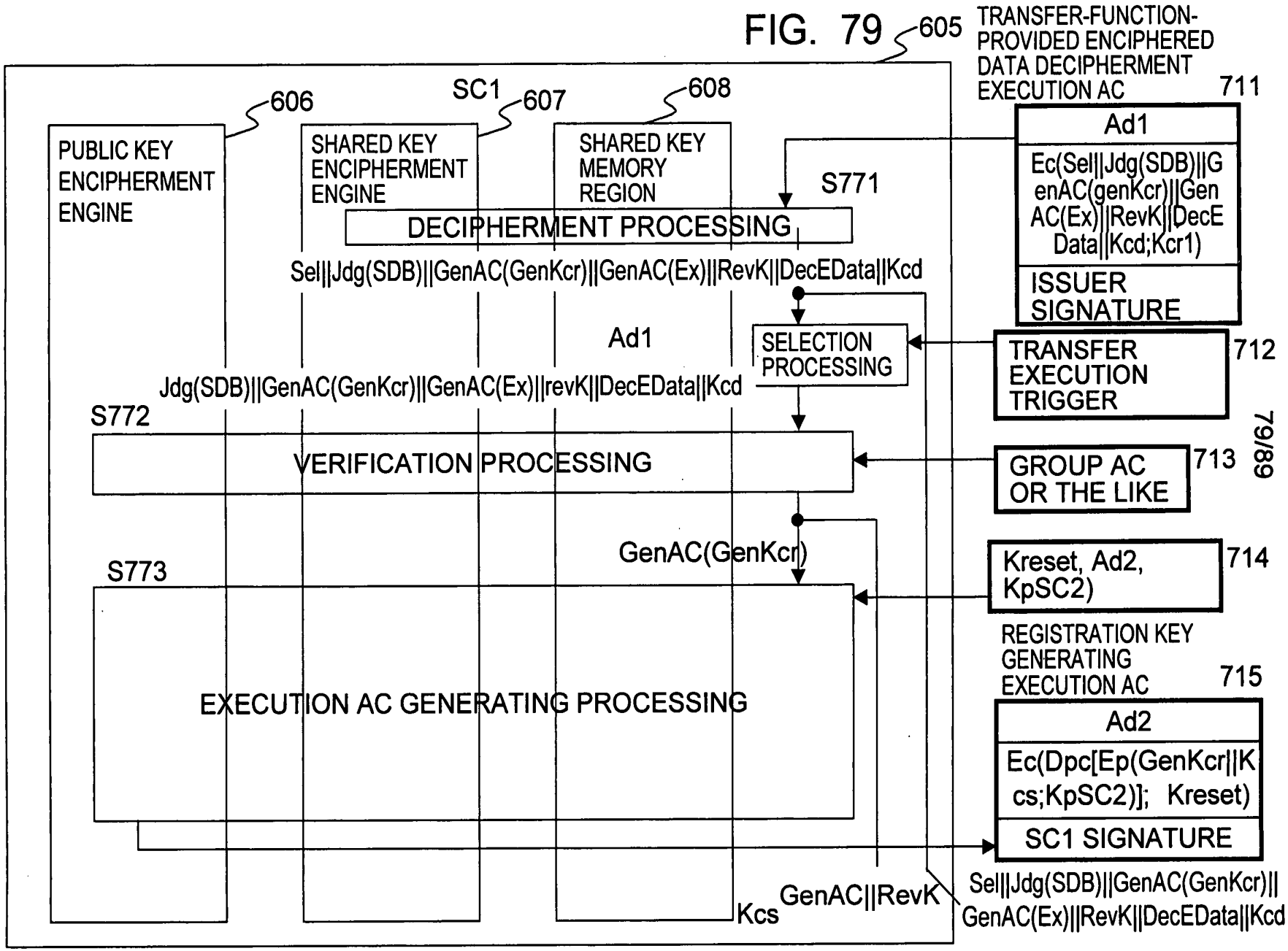


FIG. 78

FIG. 79



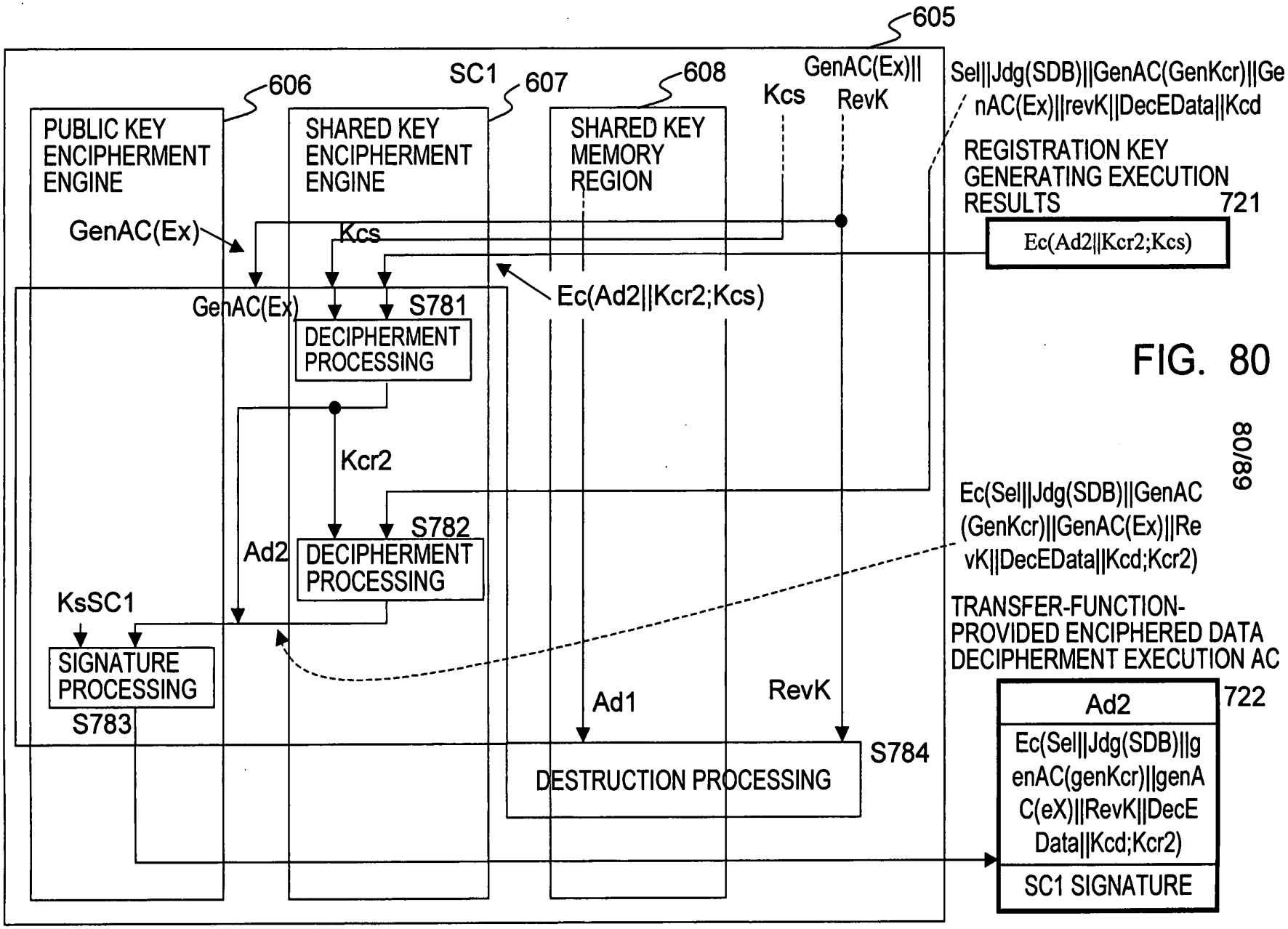


FIG. 80

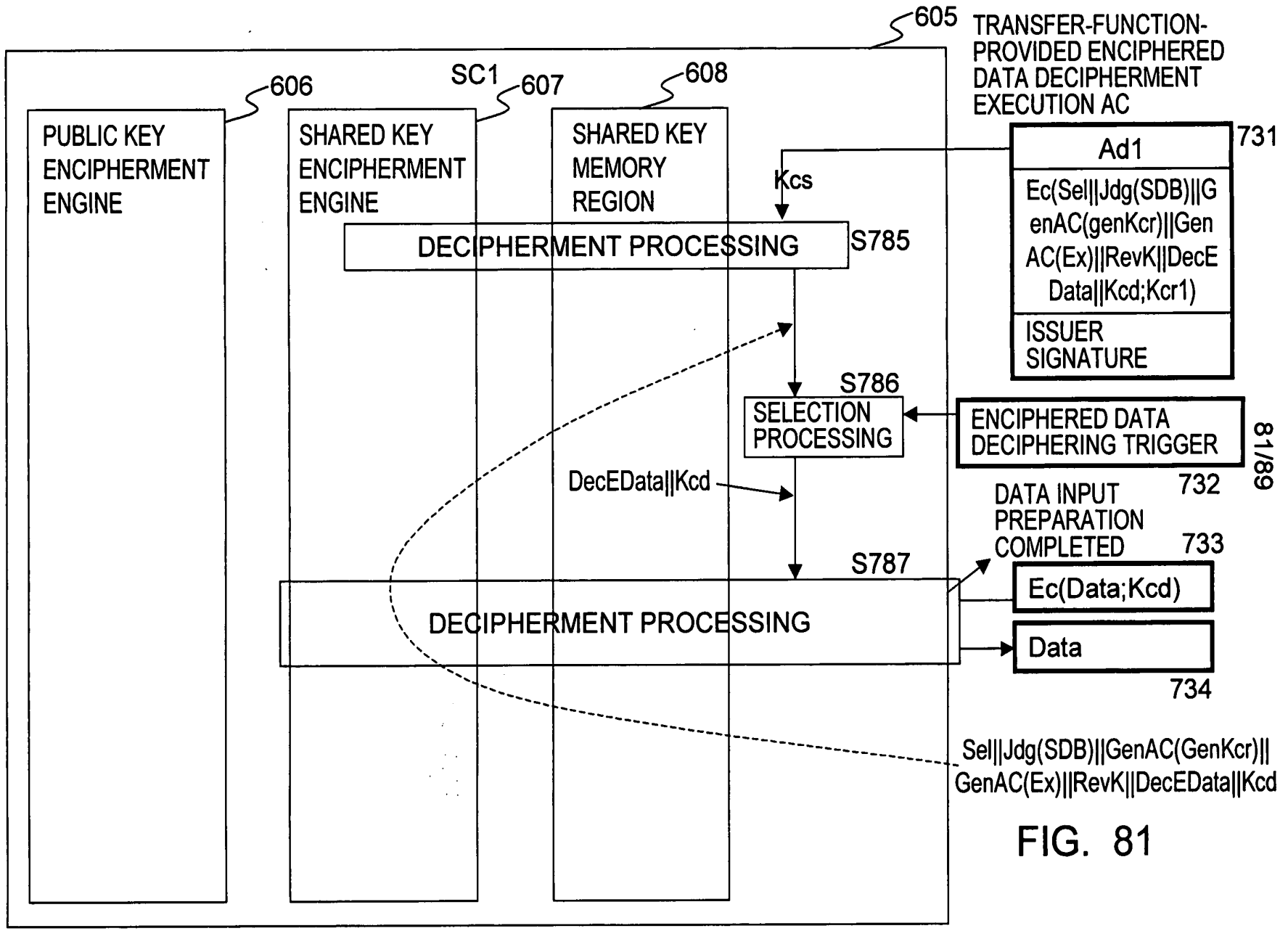
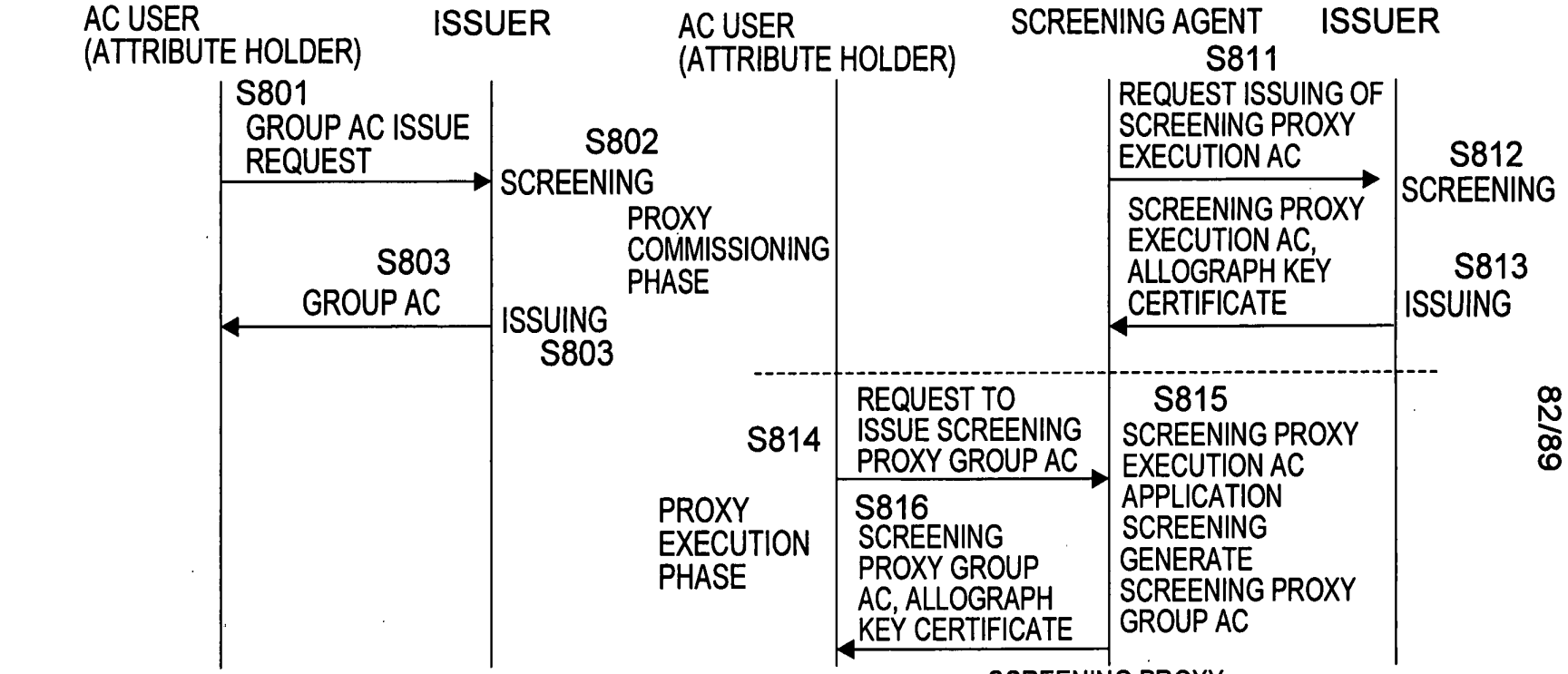


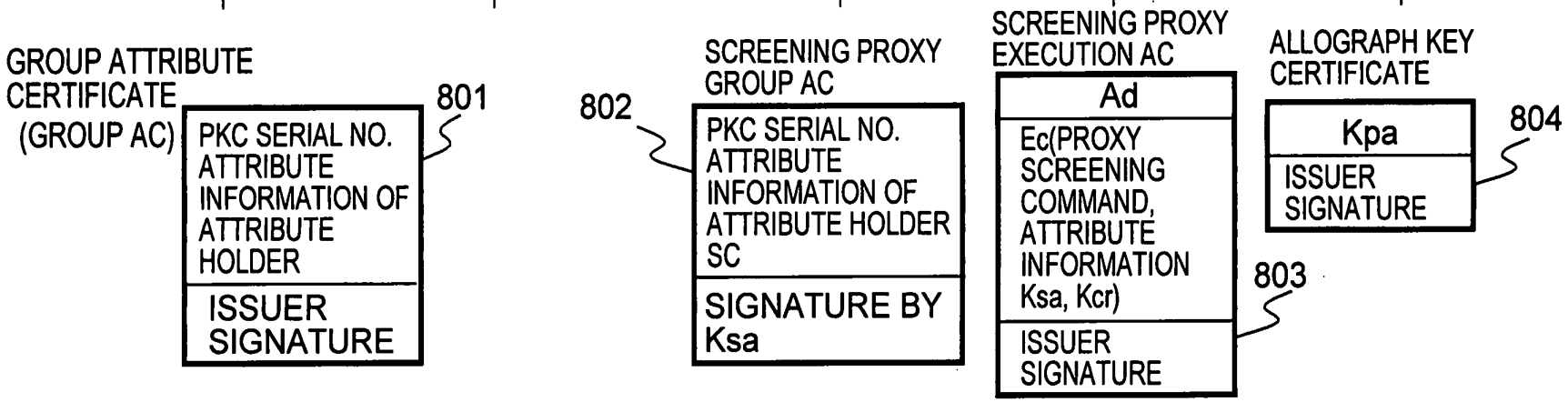
FIG. 81

(a) ISSUING CONFIGURATION FOR NORMAL ATTRIBUTE CERTIFICATE (GROUP AC)

(b) ISSUING CONFIGURATION FOR ATTRIBUTE CERTIFICATE (GROUP AC) APPLYING SCREENING PROXY EXECUTION ATTRIBUTE CERTIFICATE

FIG. 82





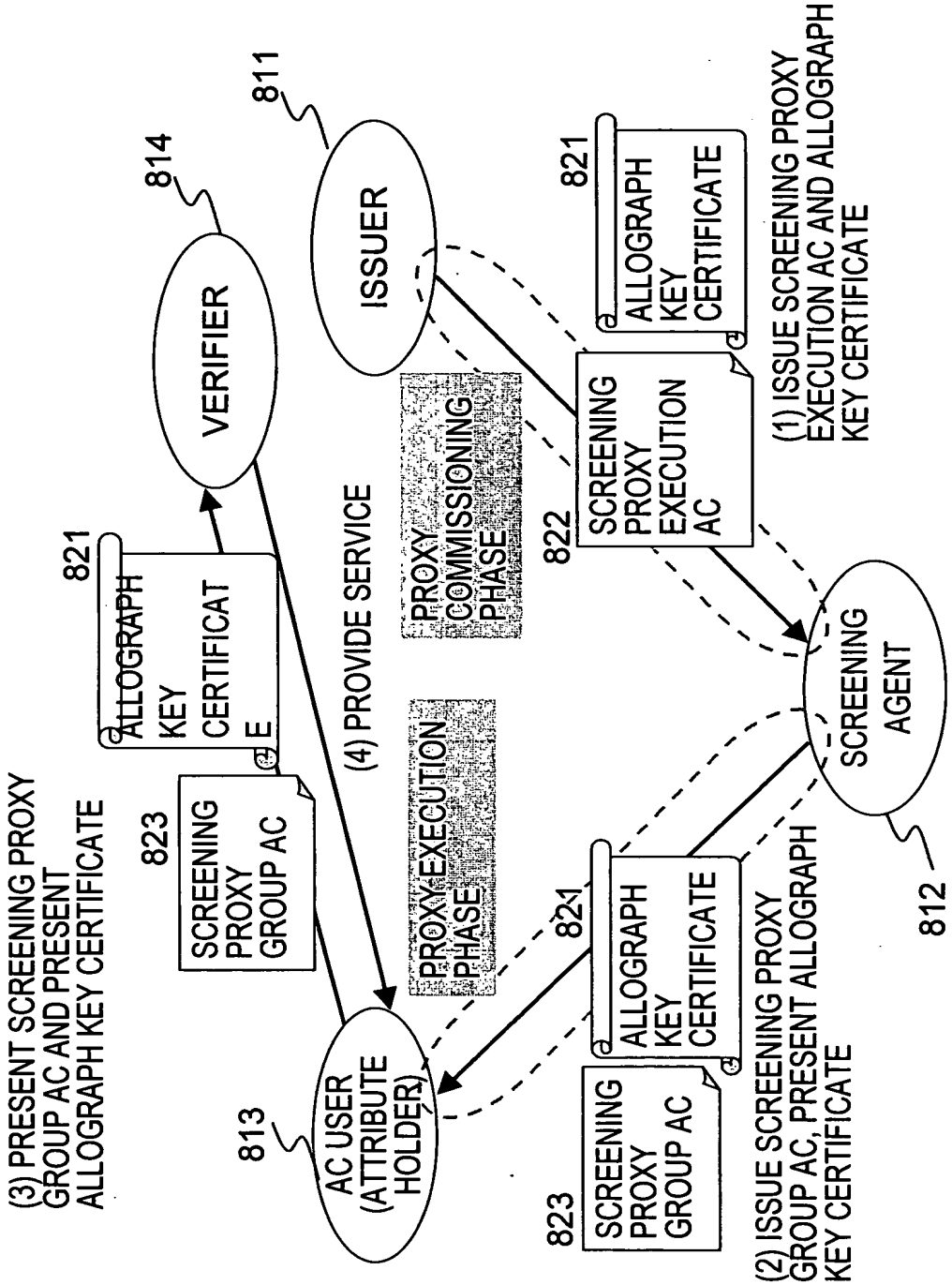

811
ISSUER
814
VERIFIER
821
ALLOGRAPH KEY CERTIFICATE
822
SCREENING PROXY EXECUTION AC
(1) ISSUE SCREENING PROXY EXECUTION AC AND ALLOGRAPH KEY CERTIFICATE
PROXY COMMISSIONING PHASE
(4) PROVIDE SERVICE
821
ALLOGRAPH KEY CERTIFICAT E
823
SCREENING PROXY GROUP AC
(3) PRESENT SCREENING PROXY GROUP AC AND PRESENT ALLOGRAPH KEY CERTIFICATE
PROXY EXECUTION PHASE
SCREENING AGENT
812
813
AC USER (ATTRIBUTE HOLDER)
821
ALLOGRAPH KEY CERTIFICATE
823
SCREENING PROXY GROUP AC
(2) ISSUE SCREENING PROXY GROUP AC, PRESENT ALLOGRAPH KEY CERTIFICATE

FIG. 83

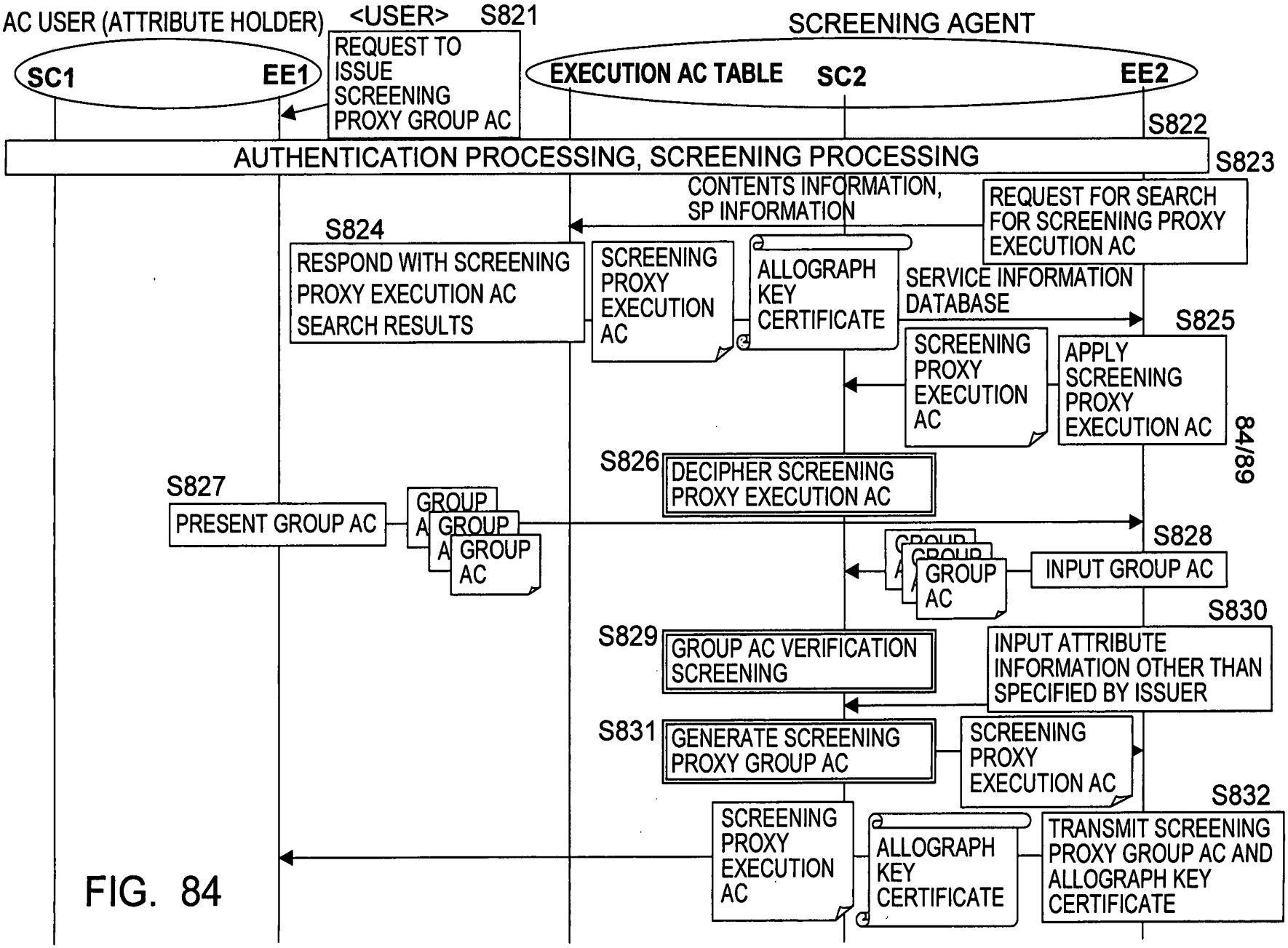


FIG. 84

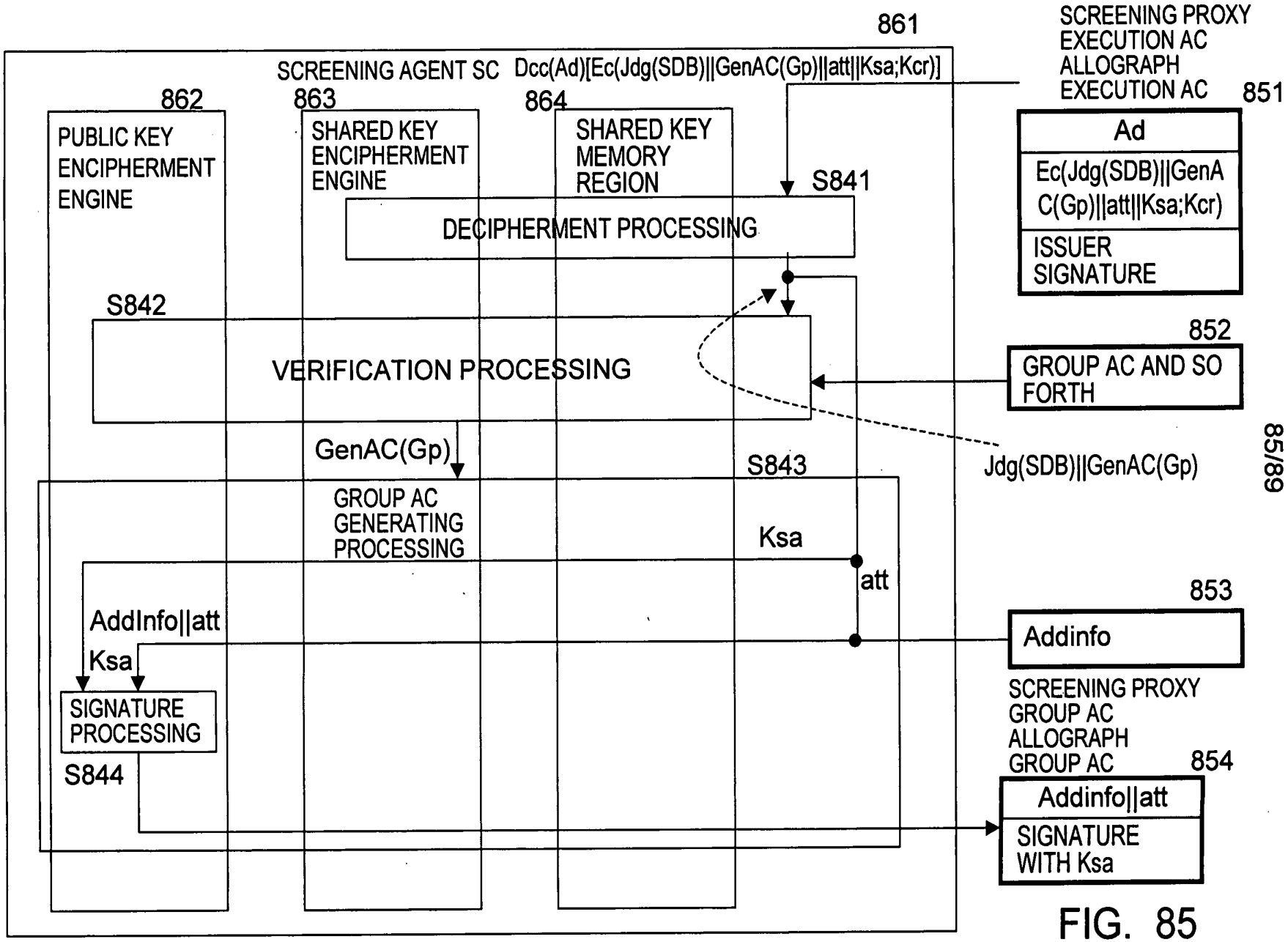


FIG. 85

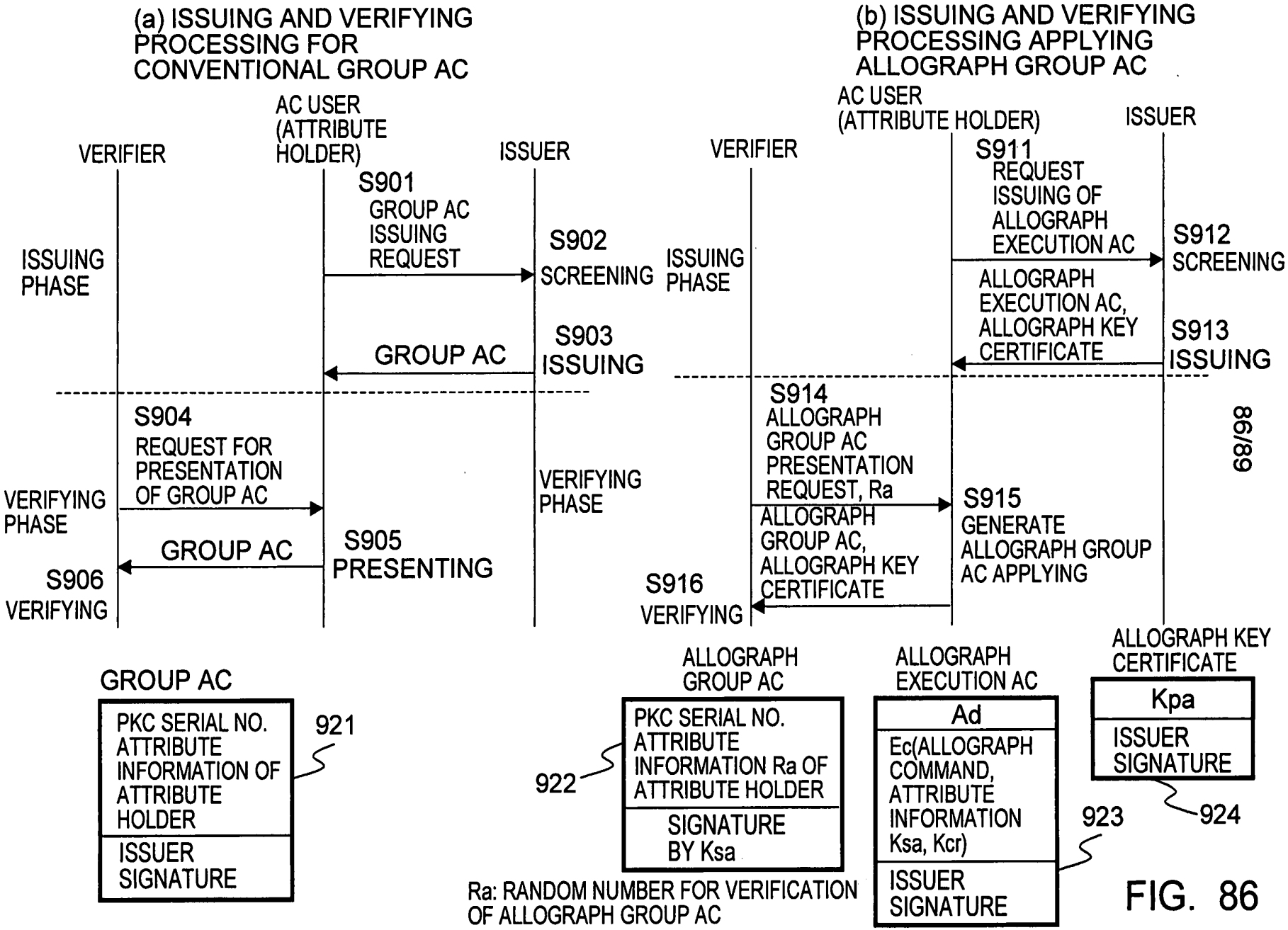


FIG. 86

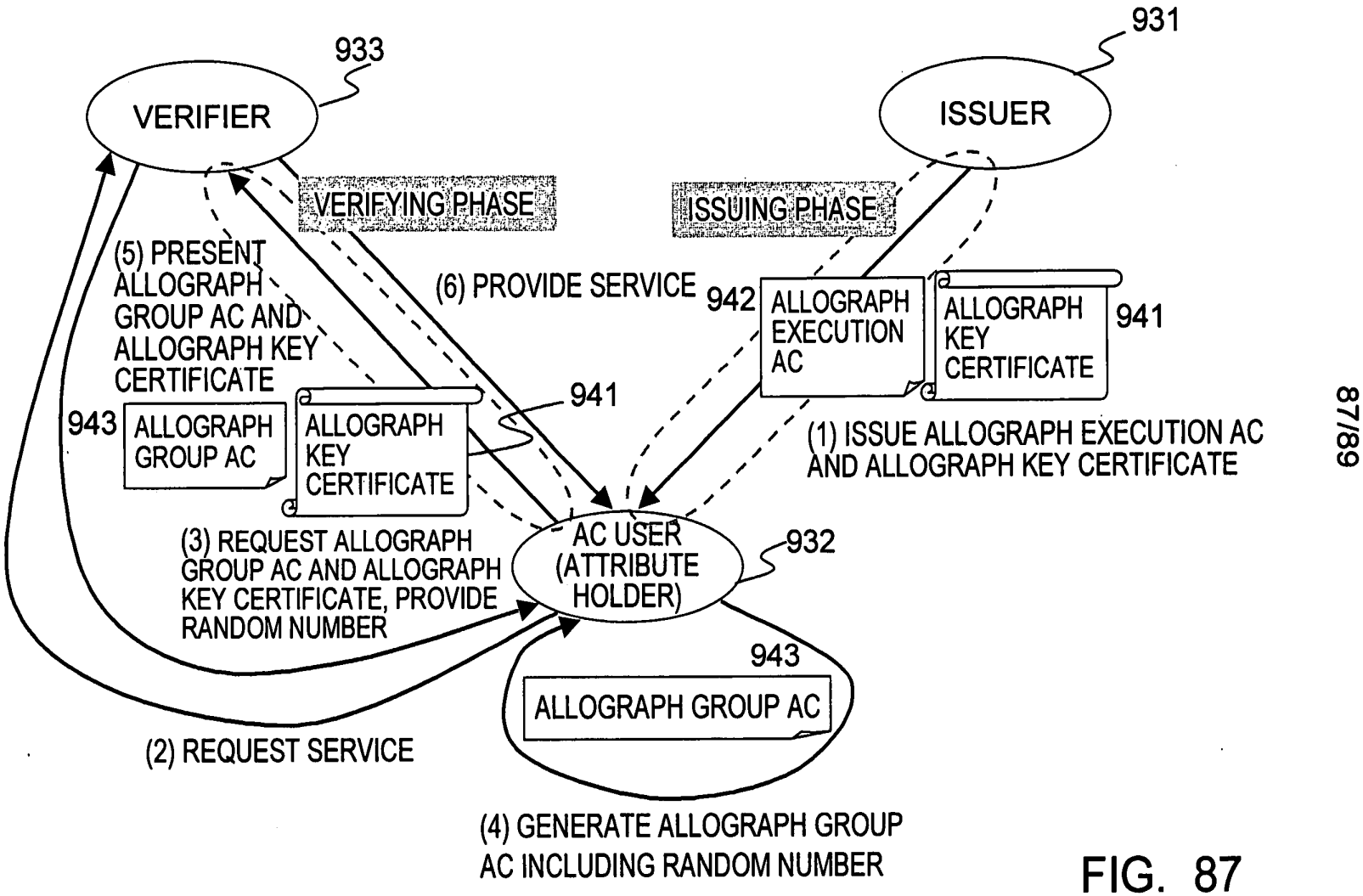


FIG. 87

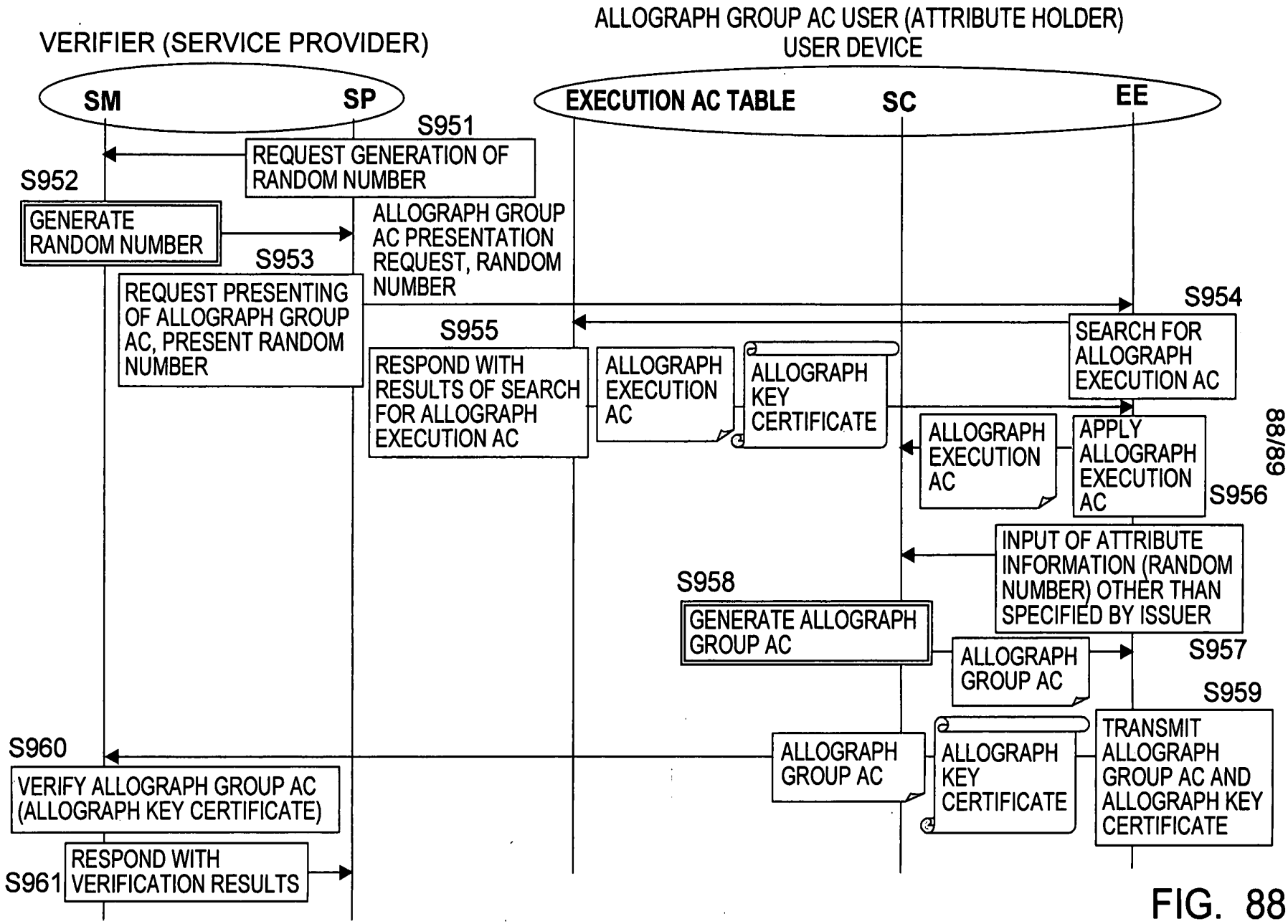


FIG. 88

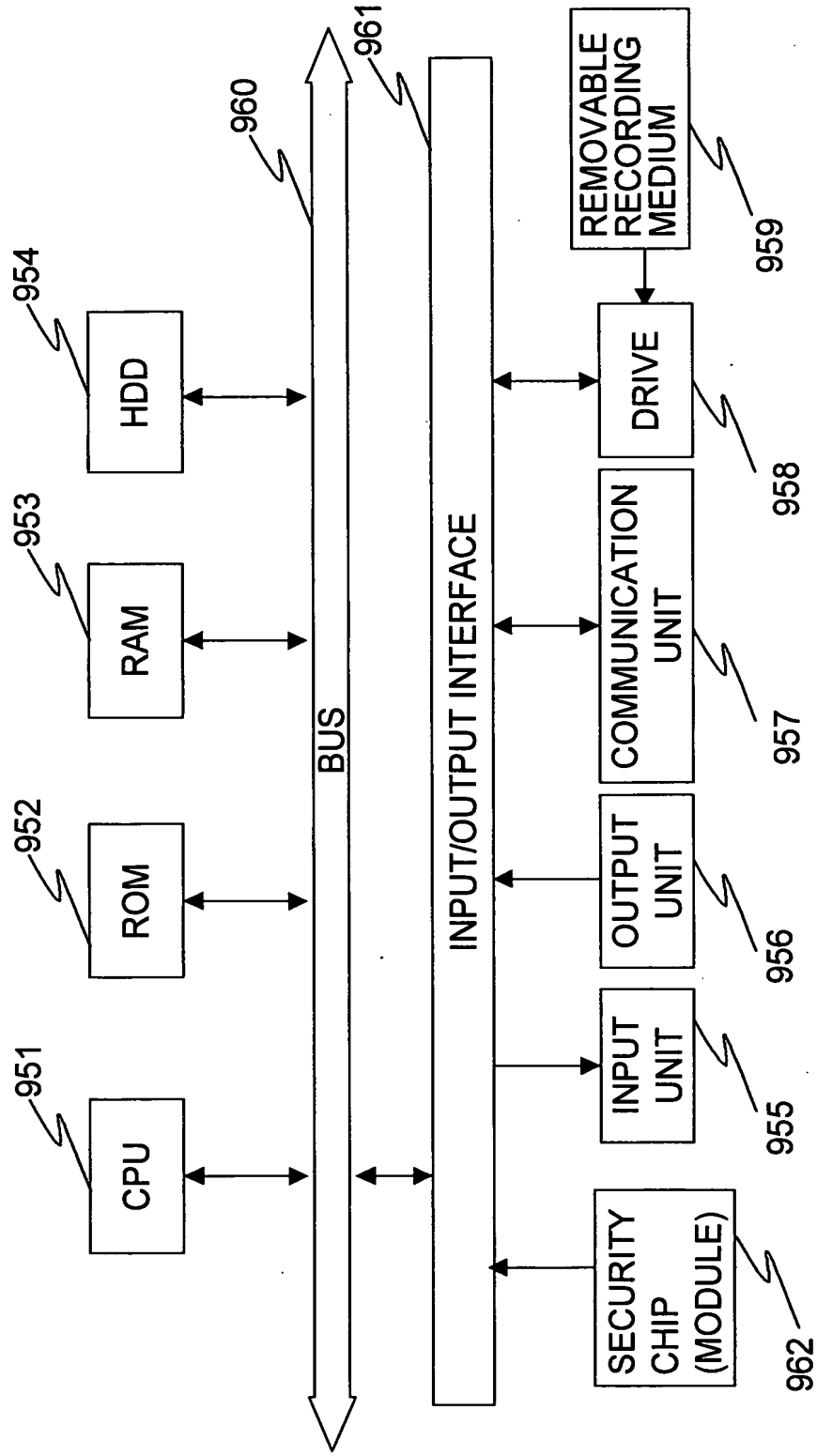

951
CPU
952
ROM
953
RAM
954
HDD
960
BUS
961
INPUT/OUTPUT INTERFACE
955
INPUT UNIT
956
OUTPUT UNIT
957
COMMUNICATION UNIT
958
DRIVE
959
REMOVABLE RECORDING MEDIUM
962
SECURITY CHIP (MODULE)

FIG. 89